On the Development of Novel Encryption Methods for Conventional and Biometric Images

Bibhudendra Acharya

Department of Electronics and Communication Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

On the Development of Novel Encryption Methods for Conventional and Biometric Images

Dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Electronics and Communication Engineering

by

Bibhudendra Acharya

(Roll- 50709003)

under the guidance of

Prof. Sarat Kumar Patra

&

Prof. Ganapati Panda

Department of Electronics and Communication Engineering
National Institute of Technology Rourkela
Rourkela, Odisha, 769 008, India

2015

dedicated to my parents...

Department of Electronics and Communication Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India.

November 24, 2015

Certificate

This is to certify that the work in the thesis entitled ***On the Development of Novel Encryption Methods for Conventional and Biometric Images*** by ***Bibhudendra Acharya***, bearing roll number 50709003, is a record of an original research work carried out by him under our supervision and guidance in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Electronics and Communication Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Sarat Kumar Patra
Professor, NIT Rourkela

Ganapati Panda
Professor, IIT Bhubaneswar

Acknowledgement

I would like to take this opportunity to express my reverence to my supervisors Prof. S. K. Patra and Prof. G. Panda for their guidance, inspiration and innovative technical discussions all during the course of this work. I find words inadequate to thank them for enabling me to complete this work in spite of all obstacles.

I am very much thankful to Prof. K.K. Mohapatra, HOD, ECE Department for his continuous encouragement. Also, I am indebted to him who provided me all official and laboratory facilities.

My sincere thanks go to Prof. S. Meher, Dr. G.S. Rath, Prof. B. D. Subudhi, Prof. S. K. Jena and Prof. B. Majhi whose valuable suggestions helped me a lot in completing this thesis. I am grateful to Prof. T.K. Dan, Prof. U. C Pati and Prof. S. K. Behera for his valuable suggestions and comments during this research period.

In addition, let me thank all my friends Abhimanyu, Ratnakar, Pankaj, Saroj, Imroze, and Prasant for their great support and encouragement during the research period. Also, I am thankful to all the non-teaching staffs of ECE Department for their kind cooperation.

Last but not the least, I take this opportunity to express my regards and obligation to my family members for encouraging me in all expects. Finally, my heartfelt thanks to my wife Suchitra for her unconditional support and encouragement in carrying my Ph.D work.

Bibhudendra Acharya

Abstract

Information security refers to the technique of protecting information from unauthorized access, use, disclosure, disruption and modification. Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic media and transmitted across networks to other computers. Encryption clearly addresses the need for confidentiality of information, in process of storage and transmission. Popular application of multimedia technology and increasingly transmission ability of network gradually leads us to acquire information directly and clearly through images and hence the security of image data has become inevitable. Moreover in the recent years, biometrics is gaining popularity for security purposes in many applications. However, during communication and transmission over insecure network channels it has some risks of being hacked, modified and reused. Hence, there is a strong need to protect biometric images during communication and transmission. In this thesis, attempts have been made to encrypt image efficiently and to enhance the security of biometrics images during transmission.

In the first contribution, three different key matrix generation methods invertible, involutory, and permutation key matrix generation have been proposed. Invertible and involutory key matrix generation methods solves the key matrix inversion problem in Hill cipher. Permutation key matrix generation method increases the Hill system's security. The conventional Hill cipher technique fails to encrypt images properly if the image consists of large area covered with same colour or gray level. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. To address these issues two different techniques are proposed, those are advanced Hill cipher algorithm and H-S-X cryptosystem to encrypt the images properly. Security analysis of both the techniques reveals superiority of encryption and decryption of images. On the other hand, H-S-X cryptosystem has been used to instil more diffusion and confusion on the cryptanalysis. FPGA implementation of both the proposed techniques has been modeled to show the effectiveness of both the techniques.

An extended Hill cipher algorithm based on XOR and zigzag operation is designed to reduce both encryption and decryption time. This technique not only reduces the

encryption and decryption time but also ensures no loss of data during encryption and decryption process as compared to other techniques and possesses more resistance to intruder attack. The hybrid cryptosystem which is the combination of extended Hill cipher technique and RSA algorithm has been implemented to solve the key distribution problem and to enhance the security with reduced encryption and decryption time.

Two distinct approaches for image encryption are proposed using chaos based DNA coding along with shifting and scrambling or poker shuffle to create grand disorder between the pixels of the images. In the first approach, results obtained from chaos based DNA coding scheme is shifted and scrambled to provide encryption. On the other hand in the second approach the results obtained from chaos based DNA coding encryption is followed by poker shuffle operation to generate the final result. Simulated results suggest performance superiority for encryption and decryption of image and the results obtained have been compared and discussed. Later on FPGA implementation of proposed cryptosystem has been performed.

In another contribution, a modified Hill cipher is proposed which is the combination of three techniques. This proposed modified Hill cipher takes advantage of all the three techniques. To acquire the demands of authenticity, integrity, and non-repudiation along with confidentiality, a novel hybrid method has been implemented. This method has employed proposed modified Hill cipher to provide confidentiality. Produced message digest encrypted by private key of RSA algorithm to achieve other features such as authenticity, integrity, and non-repudiation

To enhance the security of images, a biometric cryptosystem approach that combines cryptography and biometrics has been proposed. Under this approach, the image is encrypted with the help of fingerprint and password. A key generated with the combination of fingerprint and password and is used for image encryption. This mechanism is seen to enhance the security of biometrics images during transmission.

Each proposed algorithm is studied separately, and simulation experiments are conducted to evaluate their performance. The security analyses are performed and performance compared with other competent schemes.

***Keywords*:Security, Image encryption, Hill cipher, Involutory key matrix, Logistic chaotic map, DNA coding, Biometrics**.

Contents

List of Figures

List of Tables

List of Abbreviations

DNA	Deoxyribo Nucleic Acid
FAR	False Acceptance Rate
FRR	False Rejection Rate
MPEG	Motion Picture Experts Group
MBE	Modified Booth Encoding
CSA	Carry Save Adder
HDL	Hardware Description Language
FPGA	Field Programmable Gate Array
BCD	Binary Coded Decimal
LUT	Lookup Table
NPCR	Number of Changing Pixel Rate
UACI	Unified Averaged Changed Intensity
PRBNG	Pseudorandom Binary Number Generator
OTP	One Time Pad
MD	Message Digest
KEM	Key Encapsulation Mechanism
DP	Discriminability-Preserving
CA	Cellular Automata
FFT	Fast Fourier Transform
FrRnWT	Fractional Random Wavelet Transform
RHT	Reversible Hidden Transform
FrWPT	Fractional Wavelet Packet Transform
GCs	Garbled Circuits
OT	Oblivious Transfers

DES	Data Encryption Standard
AES	Adavanced Encryption Standard
IDEA	International Data Encryption Algorithm
MAE	Mean Absolute Error
PSNR	Peak Signal to Noise Ratio
TRNG	True Random Number Generator
LFSR	Linear Feedback Shift Register
RSA	Rivest-Shamir-Adleman
SOC	System on Chips
PLL	Phase Locked Loop
PWM	Pulse Width Modulation
SPD	Signal Processing Designer
ESL	Electronic System Level
CLB	Configurable Logic Blocks
IOB	Input-Output Blocks
API	Application Programming Interfaces
FSL	Fast Simplex Links
CRC	Cyclic Redundancy Check
MAC	Message Authentication Code
FTP	File Transfer Protocol

Chapter 1

Introduction

Chapter 1

Introduction

In this age of universal electronic connectivity, of viruses and hackers, electronic eavesdropping and electronic fraud, data security is very important at all time. Two trends have come together to make the topic of this thesis work of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of organizations and individuals on the information storage and data communication using these systems. This, in turn, has led to a increased awareness on the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of computer and network security have matured, leading to the development of practical, readily available applications to enforce network security. Two techniques of data security widely used today are cryptography and steganography. Cryptography is the practice and study of techniques for secure communication. Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. But the focus in this thesis is on cryptography.

Cryptography is the study of secret (crypto-) writing (-graphy). It is the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form. With advances in the field of cryptography; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances.

Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives-when we sign our name to some document for instance and, as we

move to a world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation of a particular time. These cryptographic mechanisms can be used to control access to a shared disk drive, a high security installation, or a pay-per-view TV channel. The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow us to pay using electronics money, to prove we know certain information without revealing the information itself, and to share a secret quantity in such a way that a subset of the shares can reconstruct the secret. While modern cryptography is growing increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some secret knowledge such as decrypting an encrypted message or signing some digital document [1, 2].

Cryptographic systems are generally classified along three independent dimensions [1, 3] :

1. **Type of operations used for transforming plaintext to ciphertext:** All encryption algorithms are based on two general principles. One is substitution, in which each element in the plaintext is mapped into another element and other one is transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.

2. **The number of keys used:** If both sender and receiver use the same key, the system is referred to as symmetric or single key or secret key conventional encryption. If the sender and receiver each uses a different key, the system is referred to as asymmetric or two key or public key encryption.

3. **The way in which the plaintext is processed:** A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptography deals with developing methods for taking a legible, readable plaintext, and transforming it into an unreadable form. The main purpose of

cryptography is secure transmission and storing of sensitive information. The process of transforming a plaintext to ciphertext is called encryption. The reverse process of converting a ciphertext to plaintext is called decryption. Protecting information is an important problem. Four security requirements for cryptography are [1]:

- **Authentication:**The process of identifying an individual.
- **Privacy/Confidentiality:** It ensures that the information will be used or read by intended user.
- **Integrity:** Integrity, in terms of data and network security, is the assurance that the information can only be accessed or modified by those authorized to do so. Information cannot be altered in storage, or in transit between the sender and the intended receiver, without the alteration being detected.
- **Non-repudiation:** A mechanism to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

The terms cryptographic algorithms and ciphers are used interchangeably in the rest of the thesis. The message to be encrypted is called a plaintext and the output of the encryption process is called a ciphertext. The following are the desired properties of a good cipher:

- Large size key to resist brute-force search.
- Fast encryption process.
- Published and reviewed algorithm: Ensuring that security depends entirely on the secrecy of key but not depend on the algorithm secrecy. (It implies that key or plaintext cannot be obtained from ciphertext just by going through the algorithm of encryption method).
- Resistance to chosen-plaintext attack: Attacker cannot determine key even if attacker can choose the plaintext for encryption. It implies resistance to known-plaintext and known-ciphertext attacks.
- Resistance to distinguishing attack: It should not produce patterns in the ciphertext output.

1.1 Types of Cryptography

There are several ways of classifying cryptographic algorithms. Based on the number of keys used in encryption and decryption there are two types of cryptography:

- Symmetric cryptography or private-key cryptography
- Asymmetric cryptography or public-key cryptography

1.1.1 Symmetric Cryptography or Private-Key Cryptography:

In symmetric cryptography or private-key cryptography, same key is used for both encryption and decryption. This means that the encryption key must be shared between the two parties before any messages can be decrypted. Symmetric cryptography can be used to transmit information over an insecure public channel. It has also other uses, such as secure storage on insecure media and strong mutual authentication. Figure 1.1 shows the symmetrical cryptosystem. The advantages and disadvantages of symmetric cryptosystem are given below:

Advantages

- A symmetric cryptosystem is faster.
- In symmetric cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.
- A symmetric cryptosystem uses password authentication to prove the receiver's identity.
- A system only which possesses the secret key can decrypt a message.

Disadvantages

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

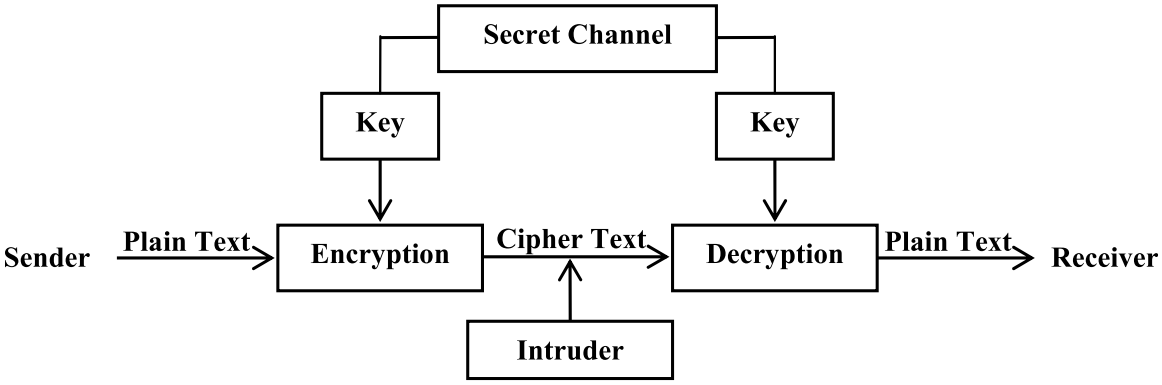


Figure 1.1: Symmetrical cryptosystem

- Cannot provide digital signatures that cannot be repudiated.

Symmetric cryptography is further subdivided into the following two types based on the amount of information it can encrypt or decrypt at a time.

- **Stream Cipher:** Stream ciphers are symmetric ciphers which encrypt one bit or one byte at a time.
- **Block Cipher:** A block-cipher divides the plaintext into blocks of bits and uses a specially constructed function which mixes a block of the plaintext with the secret key to produce a block of the ciphertext.

A stream cipher can be treated as a block cipher with a really small block size. Rueppel [4] summarizes the distinction between the block ciphers and stream ciphers as follows; "Block ciphers operate with a fixed transformation on large blocks of plaintext data; stream ciphers operate with a time varying transformation on individual plaintext digits." Block ciphers are the most widely used ciphers [1].

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1976 [5]. The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely.

1.1.2 Asymmetric Cryptography or Public-Key Cryptography:

In asymmetric cryptography or public-key cryptography, two different keys are used for encryption and decryption. One is public key and another is private key. The

private key is kept secret while the public key is distributed. Anyone can encrypt a message but only the one who knows the corresponding private key can decrypt it. Though the keys are mathematically related, it is practically not possible to retrieve the private key from the public key. The public key is used for encryption and one can decrypt the ciphertext only with the private key. Figure 1.2 shows the asymmetrical cryptosystem. The advantages and disadvantages of asymmetric cryptosystem are given below:

Advantages

- In asymmetric or public key cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
- The primary advantage of public key cryptography is increased security of the private keys do not ever need to be transmitted or revealed to anyone.
- Can provide digital signatures that can be repudiated.

Disadvantages

- A disadvantage of using public-key cryptography for encryption is speed. There are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.

To take the advantages of both categories of cryptosystem, a symmetric cryptosystem is used in addition to an asymmetric cryptosystem, if there is a need to encrypt a large message. So, traditionally, message is encrypted using the symmetric cryptosystem and the symmetric key is encrypted using the asymmetric cryptosystem which is shown in Figure 1.3.

1.2 Chaos Theory

"Chaos" means "a state of disorder". Chaos theory studies the behaviour of dynamical systems that are highly sensitive to initial conditions. A response popularly referred to as the butterfly effect. Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for such dynamical systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future

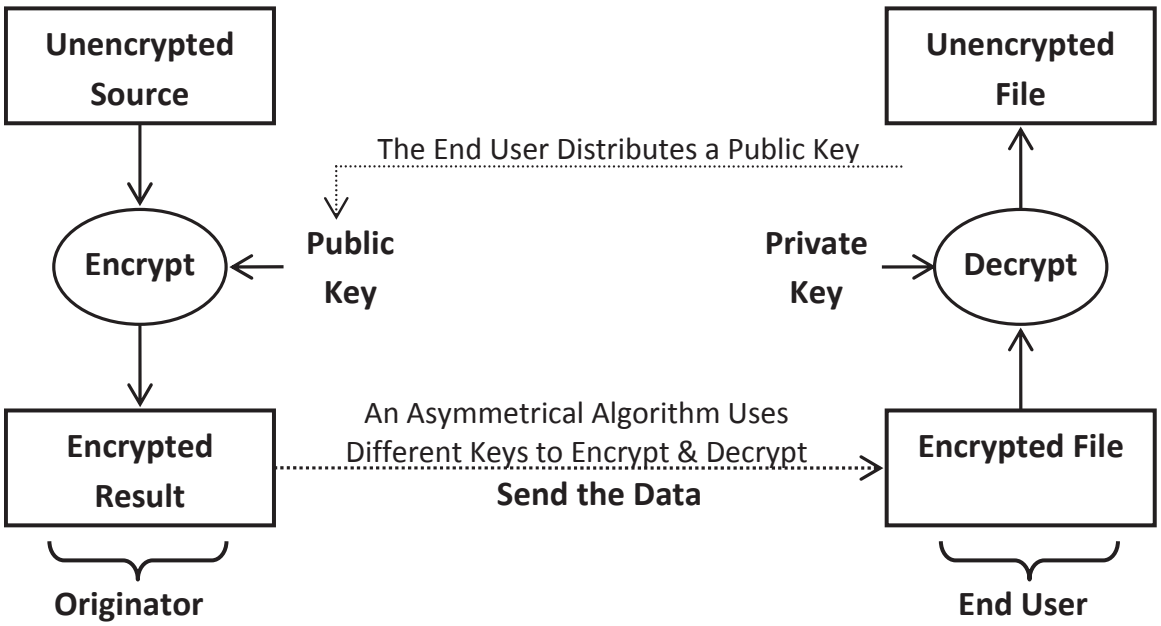


Figure 1.2: Asymmetrical cryptosystem

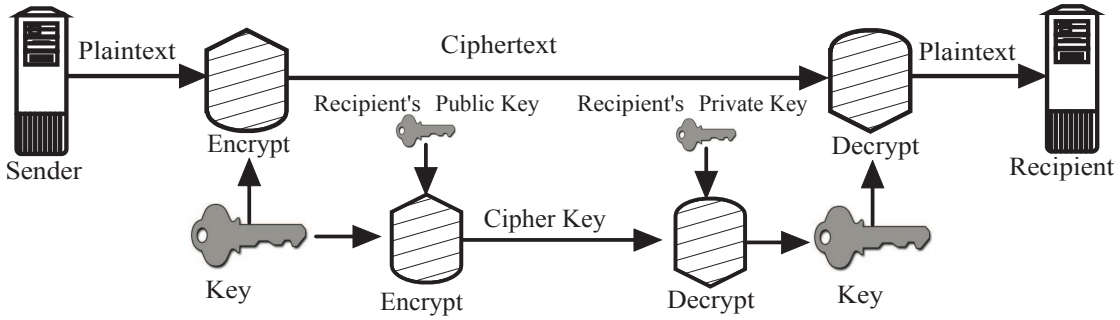


Figure 1.3: Hybrid cryptosystem

behaviour is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable. This behaviour is known as deterministic chaos, or simply chaos.

Limitations of Chaos Theory:

- The major and most significant limitation of chaos theory is the feature that defines it: sensitive to initial conditions.
- The limitations of applying chaos theory are in due mostly from choosing the input parameters. The methods chosen to compute these parameters depend on the dynamics underlying the data and on the kind of analysis intended, which

is in most cases is highly complex and not always accurate.

1.2.1 Chaotic Dynamics

For a dynamical system to be classified as chaotic, it must have the following properties:

1. It must be sensitive to initial conditions;
2. It must be topologically mixing; and
3. It must have dense periodic orbits.

1.2.2 Chaotic Map

A chaotic map is a map (= evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time parameter. Chaotic maps often occur in the study of dynamical systems. Chaotic maps often generate fractals.

1.3 DNA Cryptography

DNA cryptography is a new born cryptography, where DNA is used as information carrier and the modern biological technology is used as implementation tool. The vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, signature, and so on [6]. The main security basis depends on the restriction of biotechnology, which has nothing to do with computing power.

1.4 Poker Shuffling Theory

Image scrambling is an important technique in digital image encryption and digital image watermarking. Poker shuffling [7] is an image scrambling method which is controlled dynamically by chaotic system. Compared to other scrambling techniques such as algebraic permutations [8] and chaotic permutations [9–11], this method has properties of nonlinearity, large key space and non-analytic formula. Its scrambling

performance is satisfied and can deal with non-square image. All these features show that the Poker shuffling is more secure and efficient for image scrambling encryption.

1.5 Biometris

The term biometrics derived from the Greek words 'bios', meaning life, and 'metrikos', which means measure. Hence, biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

1.5.1 Biometric Methodologies

Biometrics can be distinguished into two major categories:

- **Physiological (or Passive) Biometrics:** Physiological biometrics refer to human characteristics which are fixed or stable such as fingerprints, hand geometry, iris pattern and, within biometrics technology, facial image and voice patterns.
- **Behavioural (or Active) Biometrics:** Behavioural biometrics measure characteristics represented by skills or functions performed by an individual at a specific time for a specific reason, for example a signature or keystroke dynamics.

Biometric technologies can also be categorised as static, dynamic, or continual. "Static" refers to measurement of a trait that requires no action at the time of verification. "Dynamic" refers to measurement of a trait while an action is taking place.

1.5.2 Biometric Template

Biometric template is a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. In other words, biometric template is a set of stored biometric features comparable directly to biometric features of a recognition biometric sample.

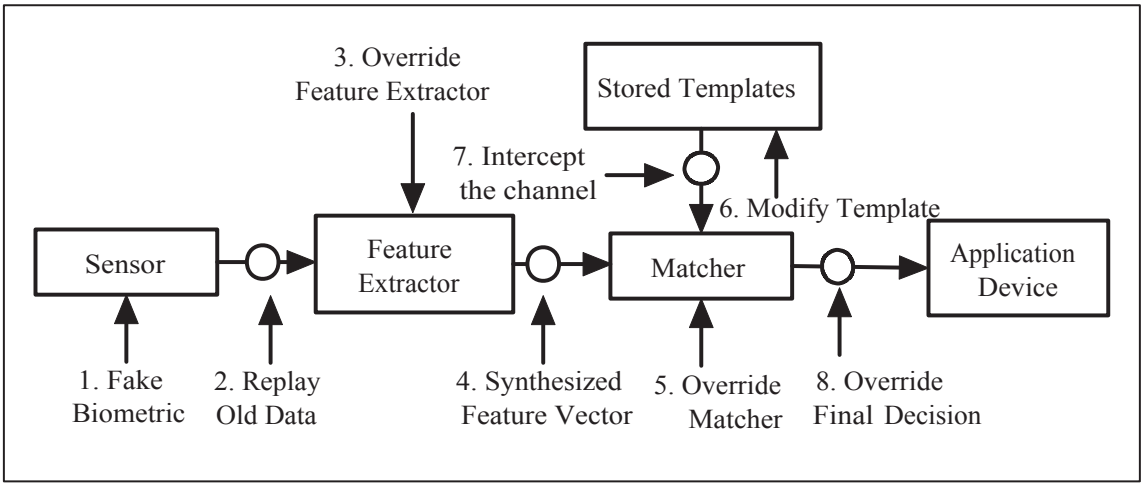


Figure 1.4: Biometric system and different points of attack

1.5.3 Biometric System

Figure 1.4 shows a biometric system model [12]. It consists of the following modules:

a. **Scanner:** The scanner module is used to scan and obtain biometric data (e.g., fingerprint, palm print, eye retinas and irises, facial patterns, voice patterns, hand veins and DNA etc.) of an individual in the form of an image, video, audio and some other signals.

b. **Feature Extractor:** The feature extractor module extracts information (or, feature set) from the signal sent by the scanner module, which represents ones identity. The feature extracted information is sent to the matcher for processing.

c. **Stored Templates:** The stored template module is a database, who stores the feature extracted information during enrolment called as templates. These templates are queried by the matcher module to find a match for the feature extracted information of the feature extractor.

d. **Matcher:** The matcher module receives feature information from the feature extractor module and compares it with the templates stored in stored template database. This module either determines or verifies the identity of an individual.

e. **Application Device:** The application device module is used to receive an answer from the matcher and take decision according to that. That means, if it receives "yes" then it grants access or if it receives "no" then it denies access.

1.5.4 Feature of Biometric System

Biometric technologies should be considered and evaluated giving full consideration to the following characteristics [13]:

- **Universality:** Every person should have the characteristic. People who are mute or without a fingerprint will need to be accommodated in some way.
- **Uniqueness:** Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.
- **Permanence:** The characteristics should not vary with time. A person's face, for example, may change with age.
- **Collectability:** The characteristics must be easily collectible and measurable.
- **Performance:** The method must deliver accurate results under varied environmental circumstances.
- **Acceptability:** The general public must accept the sample collection routines. Non-intrusive methods are more acceptable.
- **Circumvention:** The technology should be difficult to deceive.

1.5.5 Biometric System Threats:

Figure 1.4 shows different points of attacks, which are discussed in detail below [12,14].

a. **Attack at the scanner:** In this type of attack, the attacker can create a fake biometric trait, or inject an image between the sensing element and the rest of the scanner electronics. Simply means, a fake biometric is presented at the sensor.

b. **Attack on the channel between the scanner and the feature extractor:** This point of attack is known as "Replay attack". In this type of attack, the attacker intercepts the communication channel between the scanner and the feature extractor to take biometric traits and store it to somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner.

c. **Attack on the feature extractor:** In this type of attack, the attacker replaces the feature extractor module with a Trojan horse. It can be controlled by remotely. In this, the attacker sends commands to the Trojan horse to send their own selected feature values to the matcher module.

d. **Attack on the channel between the feature extractor and matcher:** This type of attack is similar to the attack on the channel between the scanner and the feature extractor. The only difference is that the attacker intercepts the communication channel between the feature extractor and the matcher to take feature values of a valid user and replay them to the matcher at a later time.

e. **Attack on the matcher:** This type of attack is similar to the attack on the feature extractor. The only difference is that the attacker replaces the matcher with a Trojan horse. This will produce either high matching score or low matching score.

f. **Attack on the system database:** In this type of attack, the attacker cracks the accounts on the database. So that the attacker can add new templates, modify the existing templates or delete templates.

g. **Attack on the channel between the system database and matcher:** This type of attack is again similar to the attack on the channel between the scanner and the feature extractor. The only difference is that the attacker intercepts the communication channel between the system database and the matcher to either steal and replay data or modify the data.

h. **Attack on the channel between the matcher and the application device:** In this type of attack, the attacker intercepts the communication channel between the matcher and the application device to replay previously submitted data or change the data.

The other attack may exist at the application level.

1.5.6 Biometric System Vulnerability

A fish bone model for categorizing biometric system vulnerabilities is shown in Figure 1.5 [12]. The failure modes of a biometric system can be classified as: intrinsic failure and failure due to an adversary attack. Intrinsic failures occur due to limitations in sensing, feature extraction or matching technologies as well as the limited discriminability of the specific biometric trait. In adversary attacks, a resourceful hacker attempts to avoid the biometric system for personal gains. Adversary attacks can be classified as: administration, non-secure infrastructure and biometric overtness [12].

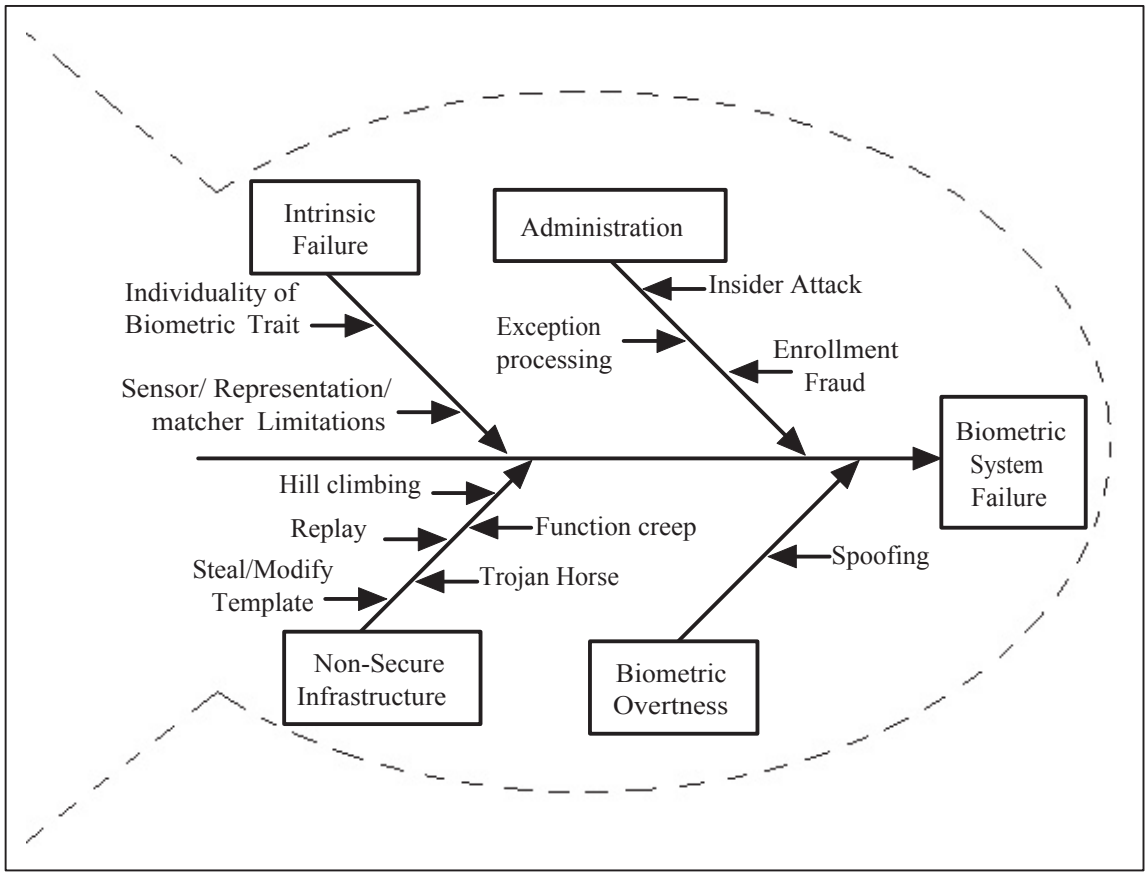


Figure 1.5: Fish bone model

a. **Intrinsic Failure:** Intrinsic failure is the security lapse due to an incorrect decision made by the biometric system. A biometric verification system can make two types of errors in decision making, namely false accept and false reject. A valid user may be falsely rejected by the biometric system due to mismatch of the user's stored template and query biometric feature sets. False accepts are usually caused by lack of individuality or uniqueness in the biometric trait.

b. **Adversary Attack:** This type of attacks occurs due to the identification and use of the loopholes in the implementation of the biometric algorithms or insecure configuration to avoid the biometric system. The adversary attacks are categorized into three main classes: administration attack, non-secure infrastructure and biometric overtness.

c. **Effects of Biometric System Failure:** When a biometric system is compromised, it can lead to two main effects : i) denial-of-service and ii) intrusion.

(i) **Denial-of-service:** it refers to the scenario where a genuine user is prevented from obtaining the service that he is entitled to. Intrinsic failures such as false reject, failure to capture and failure to acquire also lead to denial-of-service. Administrative exploitation such as modification of templates or the operating parameters (e.g. matching threshold) of the biometric system may also result in denial-of-service.

(ii) **Intrusion:** It refers to an impostor gaining illegitimate access to the system, resulting in loss of privacy (e.g. unauthorized access to personal information) and security threats (e.g. terrorists crossing borders). All the four factors that cause biometric system vulnerability, namely, intrinsic failure, administrative abuse, non-secure infrastructure and biometric overtness, can result in intrusion.

d. **Counting Adversary Attacks:** Adversary attacks generally exploit the system vulnerabilities at one or more modules or interfaces. These attacks are grouping into four categories, namely, (i) attacks at the user interface (input level), (ii) attacks at the interfaces between modules, (iii) attacks on the modules, and (iv) attacks on the template database.

1.5.7 Biometric Template Protection Schemes

An ideal biometric template protection scheme should possess the following four properties [12].

I. **Diversity:** The secure template must not allow cross matching across databases, thereby ensuring the user's privacy.

II. **Revocability:** It should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.

III. **Security:** It must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

IV. **Performance:** The biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

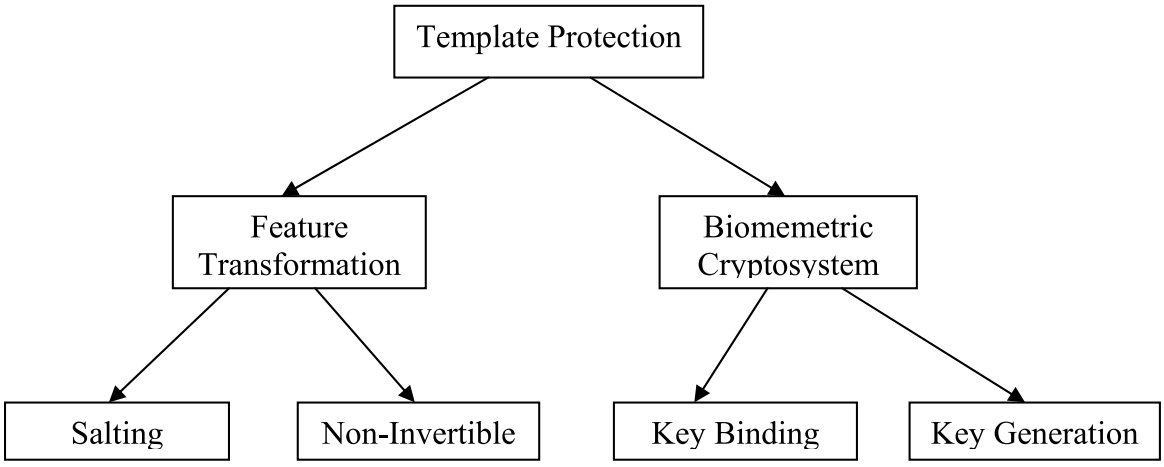


Figure 1.6: Categorization of template protection schemes

Figure 1.6 shows various template protection schemes [12]. Template protection schemes are broadly classified into feature transform and biometric cryptosystem as shown.

A. **Salting:** Salting is a template protection approach in which the biometric features are transformed using a function defined by a user-specific key or password. Since the transformation is invertible to a large extent, the key needs to be securely stored or remembered by the user and presented during authentication. This need for additional information in the form of key increases the entropy of the biometric template and hence makes it difficult for the adversary to guess the template.

B. **Non-invertible Transform:** In this approach, the biometric template is secured by applying a non-invertible transformation function to it. Non-invertible transform refers to a one-way function, F, that is " easy to compute " (in polynomial time) but "hard to invert" (given F(x), the probability of finding x in polynomial-time is small). The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set. The main characteristic of this approach is that even if the key and/or the transformed template are known, it is computationally hard (in terms of brute force complexity) for an adversary to recover the original biometric template.

C. **Key Binding Biometric Cryptosystem:** In a key binding cryptosystem, the biometric template is secured by monolithically binding it with a key within a cryptographic framework. A single entity that embeds both the key and the

template is stored in the database as helper data. This helper data does not reveal much information about the key or the biometric template, i.e., it is computationally hard to decode the key or the template without any knowledge of the user's biometric data. Usually the helper data is an association of an error correcting code (selected using the key) and the biometric template. When a biometric query differs from the template within certain error tolerance, the associated codeword with similar amount of error can be recovered which can be decoded to obtain the exact codeword and hence, recover the embedded key. Recovery of the correct key implies a successful match.

D. **Key Generating Biometric Cryptosystem:** Direct cryptographic key generation from biometrics is an attractive proposition but it is a difficult problem because of the intra-user variability. Key generating biometric cryptosystems usually suffer from low discriminability which can be assessed in terms of key stability and key entropy. Key stability refers to the extent to which the key generated from the biometric data is repeatable. Key entropy relates to the number of possible keys that can be generated. Note that if a scheme generates the same key irrespective of the input template, it has high key stability but zero entropy leading to high false accept rate. On the other hand, if the scheme generates different keys for different templates of the same user, the scheme has high entropy but no stability and this leads to high false reject rate. While it is possible to derive a key directly from biometric features, it is difficult to simultaneously achieve high key entropy and high key stability.

1.6 Literature Review

This section describes a brief review on different encryption techniques, multipliers for FPGA implementation and biometric image encryption techniques.

In 1929, Lester S. Hill developed cryptography in an algebraic alphabet called the Hill cipher [15]. It is a polygraphic substitution cipher based on linear algebra and overcomes the frequency distribution problem of Caesar cipher. In Hill cipher, the encryption is not simply based on replacing certain characters with others but, instead, on linear transformations of blocks of characters, the frequencies of each letters appearance in the language have been masked. Since the Hill cipher is strictly based on matrix multiplication and inverses, it has high speed and high throughput.

This linearity, however, is still subject to simple attacks. If an attacker intercepted enough plaintext and ciphertext pairs, a linear system could be set up to calculate the encryption matrix and also it cannot encrypt the images properly if the image consists of large areas covered with same color or gray level [5, 16–20].

Several solutions to these problems as means of securing the Hill cipher have been proposed. In 2000, one such solution Saeednia [21] addressed by using dynamic key matrix, which is obtained by random permutations of rows and columns from master key. Here, the number of dynamics keys is $m!$ where m is the number of rows and columns of the dynamic key matrix. But Saeednia's scheme computationally time intensive due to matrix computation. To overcome the drawbacks of Saeednia's scheme, in 2004, a more secure cryptosystem with a one-way hash function was proposed by Lin et al. [22]. However, hash function usage makes this technique computationally hard. In 2007, another modification was proposed by Chefranov et al. [23] which is same as Saeednia's secure Hill cipher scheme but it does not transfer permutations instead both sender and receiver uses pseudo random permutation generator. Sender and receiver share secret SEED value which is used to generate random number.

In 2009, Rushdi et al. [24] suggests a new technique in Hill cipher algorithm aimed to overcome the Hill's major problem- noninvertible key matrix. This paper also suggested enhancement to the security of Hill cipher against known plaintext attack because all steps in Hill cipher depend on linear algebra calculation. This was made possible by using public key idea and key generating depending on various options without linear algebra steps which makes it difficult for the attacker to get the key.

Again some modifications were proposed by researchers to improve the encryption quality and better hiding of all features of the images containing large single colour areas. These modification were based on eigenvalues [25], pseudo random eigenvalues [26], and generalized permutation [27].

In 1982, systolic architectural concept was developed at the Carnegie-Mellon University, by Kung [28]. Systolic architecture is a general methodology for mapping high-level computations into hardware structures resulting in cost-effective, high performance special-purpose systems for a wide range of problems.

Finite fields have been used for numerous applications including error-control coding and cryptography. The design of efficient multipliers, dividers, and exponentiators for finite field arithmetic is of great practical concern. In 1998, Jain et al. [29] explored and classified algorithms for finite field multiplication, squarring, and

exponentiation into least significant bit first (LSB-first) scheme and most significant bit first (MSB-first) scheme, and implement these algorithms using semisystolic arrays. For finite field multiplication (for programmable as well as fixed field order) and exponentiation, we conclude that LSB-first algorithms are more efficient as their basic cells have less critical path computation time. Another advantage of LSB-first scheme is its capability in achieving substructure sharing among multiple operations, which could lead to savings in hardware when these arithmetic units are used as building blocks for a large system. For finite field squarring operation, it turns out that the MSB-first algorithm is more efficient as it leads to simpler architectures. Bit-level pipelined semisystolic architectures utilize broadcast signals. As a result, these require lesser number of latches and leading to much lower latency than the corresponding systolic array, with the same cycle time (the computation time in one basic cell). Efficient VLSI implementation of semisystolic multipliers, squarers and exponentiators are designed and compared with existing architectures.

Motion estimation constitutes a significant computational part of video compression standards such as MPEG4. In 2007, Saldana et al. [30] focuses on the development of a reconfigurable systolic-based architecture implementing the full search block matching algorithm which is highly computing intensive requiring a large bandwidth to obtain real-time performance.

In 1951, Booth [31] proposed a technique whereby binary numbers of either sign may be multiplied together by a uniform process which is independent of any foreknowledge of the signs of these numbers. He presented an algorithm to multiply two signed, two's complement numbers. This algorithm has been extended for higher radix operands for computational speedup. However, for certain size operands, correction shifts have to be performed on the product produced by the Booth algorithm in order to obtain a correct product. This paper presents a modification of the Booth algorithm that does not need any correction shifts for any operand size and for any radix that is a power of 2.

In 1993, Fadavi-Ardekani [32] presented the architecture and the design method of an $M-$bit by $N-$bit Booth encoded parallel multiplier generator. A new algorithm for reducing the delay hide the branches of the Wallace tree section was explained. The final stage of adding two $N+M-1-$bit numbers was done by an optimal carry select adder stage. The algorithm for optimal partitioning of the $N+M-1-$bit adder was also presented.

In 1993, Madrid et al. [33] presented a modified Booth algorithm for operand

sizes that are a power of 2. This modified algorithm requires correction cycles after the original Booth algorithm has been completed. In 1994, Katti [34] presented an algorithm which was not restricted to operand sizes that are powers of 2 but achieved the work without correction cycles.

In 2003, Jou et al. [35] proposed a low-error reduced-width Booth multiplier using a proper compensation vector dependent on the input data. The compensation value thus obtained was adaptively adjusted when the input data are different.

The conventional Modified Booth Encoding (MBE) generates an irregular partial product array because of the extra partial product bit at the least significant bit position of each partial product row. In 2009, Kuang et al. [36] proposed a simple approach to generate a regular partial product array with fewer partial product rows and negligible overhead, thereby lowering the complexity of partial product reduction and reducing the area, delay, and power of MBE multipliers.

Designing multipliers that are of high-speed, consuming low power, and/or regular in layout is of substantial research interest. Many attempts have been made to reduce the number of partial products generated in a multiplication process one of them is Wallace tree multiplier. Wallace tree CSA structures have been used to sum the partial products reduced time. In 2011, Chaudhary et al. [37] proposed a 8×8 bit modified Wallace tree multiplier. Wallace high-speed multiplier uses full-adders and half-adders, 4:2 compressor, 3:2 compressor in their reduction phase. Minimizing the number of half-adders used in a multiplier reduction reduced the complexity. A modification to the Wallace reduction is presented that the delay is the same as for the conventional Wallace reduction.

Speed of the multiplier can be enhanced by reducing the process of generating partial products. Many attempts have been made to reduce the number of partial products generated in a multiplication process one of such work by Wallace used tree multiplier. Wallace tree CSA structures have been used to sum the partial products in reduced time. In 2012, Gahlan et al. [38] investigated and evaluated Wallace tree compressor. Speed of traditional Wallace tree multiplier can be improved by using compressor techniques. Gahlan proposed Wallace tree constructed by traditional method with the help of compressor techniques such as 4:2 compressor, 5:2 compressor, 6:2 compressor, and 7:2 compressor thereby minimizing the number of half-adders used in a multiplier leading to reduced complexity.

In 2012, Rao et al. [39] proposed a Wallace tree multiplier using Booth recoder. It is an improved version of tree based Wallace tree multiplier architecture. This

architecture aims at additional reduction of latency and area of the Wallace tree multiplier. This is accomplished by the use of Booth algorithm and compressor adders. The coding was done in verilog HDL and synthesized for Xilinx Virtex 6 FPGA device. The result demonstrated proposed architecture to be around 67 percent faster than the existing Wallace-tree multiplier, 53 percent faster than the Vedic multiplier, 22 percent faster than the radix-8 Booth multiplier, 18 percent faster than the radix-16 Booth multiplier. In terms of area also, this multiplier was also found to be efficient.

In 2012, Kumar et al. [40] proposed the design of high speed Vedic multiplier using the techniques of ancient Indian Vedic mathematics that have been modified to improve performance. Vedic mathematics is the ancient system of mathematics which has a unique technique of calculations based on 16 sutras. The work has proved the efficiency of Urdhva Triyagbhyam Vedic method for multiplication which strikes a difference in the actual process of multiplication itself. It enables parallel generation of intermediate products, eliminates unwanted multiplication steps with zeros and scaled to higher bit levels using Karatsuba algorithm with the compatibility to different data types. Urdhva Triyagbhyam Sutra is most efficient sutra (algorithm), giving minimum delay for multiplication of all types of numbers, either small or large. Further, the verilog HDL coding of Urdhva Triyagbhyam Sutra for 32×32 bits multiplication and their FPGA implementation by Xilinx synthesis tool on Spartan 3E kit have been implemented. Around the same time, Saha et al. [41] proposed decimal number system multiplication technique based on Vedic mathematics. Improvement in speed was achieved through stage reduction by "Nikhilam Navatascaramam Dasatah (NND)" (all from 9 and last from 10) which was adopted from Vedas, during multiplication. Binary Coded Decimal (BCD) methodology was incorporated with Vedic mathematics, to implement such multiplier for practical VLSI applications. BCD implementation of Vedic multiplier ensures the stage reduction for decimal number, hence substantial reduction in propagation delay compared with earlier reported one, has been investigated. Almost 26% improvement in speed w.r.t. earlier reported decimal multiplier had been achieved.

Matrix multiplication is the kernel operation used in many image and signal processing applications. In 2010, Qasim et al. [42] presented the design and Field Programmable Gate Array (FPGA) implementation of matrix multiplier architectures for use in image and signal processing applications. The designs were optimized for speed. Constant multipliers were widely used to implement the multiplication of signals by a constant coefficient.

In 2013, Hormigo et al. [43] presented a self-reconfigurable constant multiplier suitable for LUT-based FPGAs able to reload the constant in runtime. The pipelined architecture presented was scalable to any multiplicand and constant sizes, for unsigned and signed representations. These could be reprogrammed in 16 clock cycles, equivalent to less than 100 ns in current FPGAs. This parameter is significantly smaller than FPGA partial configuration. The presented approach was more efficient in terms of area and speed when compared to generic multipliers, achieving up to 91% area reduction with 102% speed improvement for the case-study considered. The power consumption of the proposed multipliers was in the range of those of slice-based multipliers commercially available.

In 2002, Pillmeier [44] examines design alternatives for barrel shifters that perform the following functions: shift right logical, shift right arithmetic, rotate right, shift left logical, shift left arithmetic, and rotate left. Four different barrel shifter designs were analyzed here in terms of area and delay for a variety of operand sizes. In 2012, Asati et al. [45] designed MUX based barrel shifter circuits which was implemented in $0.6\mu m$, N-well CMOS process using three different logic design styles, namely, optimized static CMOS, transmission gate (TG) CMOS and dual rail domino CMOS logic. The proposed barrel shifter architecture implementation showed large reduction in the propagation delay.

Sastry et al. proposed some modified Hill cipher algorithms. At first, in 2005, he published a paper "On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher" [46]. Here plaintext matrix is not thoroughly mixed with the key matrix leading to presence of diffusion, subsequently to develop a cipher for a large block size, In 2006, Sastry et al. [47] developed a block cipher, wherein the key matrix and the plaintext vector are converted into binary bits and mod 2 operations to obtain the ciphertext. In this, a thorough mixing of the elements of the key matrix and the plaintext matrix lead to a cipher, which cannot be broken by any cryptanalytic attack. For strengthening the cipher, in 2007, Sastry et al. [48] modified the Hill cipher by using linear congruences. In this scheme two secret keys were used: one is the key matrix and another one is the key involving the constants occurring in the linear congruences. These two keys were termed as outer key and inner key respectively. Out of this the inner key played a very significant role in strengthening the cipher.

In 2007, Sastry et al. [49] proposed another method which is "Modified Hill Cipher with Interlacing and Iteration". It provided more robustness towards known plaintext attacks. In this a block cipher was developed by using a large key matrix. The

primary concept was interlacing of the binary bits of the plaintext vectors, occurring in the plaintext matrix. Here, the multiplication of the plaintext with the key causes diffusion and the interlacing of the plaintext at various stages of iteration causing confusion in an effective manner. The key size taken was very large so that data cannot be extracted from ciphertext easily. Also due to Avalanche effect, change in one bit of plaintext adds a number of extra bits to the ciphertext and hence opponent could not get this change easily.

Around the same time, Sastry et al. [50] published a paper "Modified Hill Cipher with Key Dependent Permutation and Circular Rotation", where a cipher is developed which involves different types of transformations such as permutation and circular rotation in addition to matrix multiplication and modular arithmetic. This work used iteration in order to enhance the strength of the cipher which was expected to be a very strong. The strength of the cipher increased enormously as the permutation and the rotation are key dependent, and they include a lot of confusion into the structure of the plaintext at various stages of the iteration.

In 2008, Sastry et al. [51] proposed modification with interlacing and iteration by developing a block cipher, wherein the block is taken in the form of a large matrix. The cipher under consideration can be applied to a plaintext of any size (with padding, if needed) and the strength of the cipher is quite significant as interlacing is causes a lot of transposition in the elements of the plaintext.

In 2010, Sastry et al. [52] proposed a modified Hill cipher involving interweaving (transposition of the binary bits of the plaintext characters belonging to the neighbouring rows and columns) and iteration. In this, the multiplication of the plaintext with the key matrix, the interweaving and the iteration cause a lot of diffusion and confusion. Here, a strong block cipher was developed, whose key length was seen to be significantly large.

In 2014, Naskar et al. [53] proposed a symmetric image encryption technique based on bit-wise operation (XORing and Shifting). The basic idea was block ciphering (size of each block is 4 bytes) technique to cipher the secret bytes, after that ciphered bytes are again shuffled among N positions (N is the size of secret file). The scheme was a combination of substitution as well as transposition techniques which provided additional protection of the secret data.

The Number of Pixel Changing Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks.

Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks. However, it is not clear how high NPCR/UACI is such that the image cipher indeed has a high security level. In 2011, Wu et al. [54] analyzed this problem by establishing a mathematical model for ideally encrypted images and then derived expectations and variances of NPCR and UACI under this model.

In general, the term 'chaos' refers to a situation or place of great disorder and unpredictability. According to the Merriam-Webster dictionary "A state of utter confusion". In 2003, Belkhouche et al. [55] used one-dimensional chaotic map for binary images encryption. In order to perform pixel value permutation, the approach used the diffusion property of chaotic maps, where local information was spread out. Comparison in terms of the correlation between the initial image and the transformed images was provided for different degrees of chaocity which corresponds to different values of positive Lyapunov exponent. It was also shown that the sensitivity to initial state played an important role in chaotic encryption.

In 2006, Gu et al. [56] proposed a strong image encryption algorithm which used both permutation and substitution methods together. An optimized treatment and a cross-sampling disposal have been introduced for enhancing the irregular and pseudorandom characteristics of chaotic sequences. In 2006, Xiao et al. [57] proposed a scheme of using two chaotic systems based on the thought of higher secrecy of multi-system. One of the chaotic systems was used to generate a chaotic sequence. Then this chaotic sequence was transformed into a binary stream by a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, the pixel values of a plain image have been modified randomly using the binary stream as a key stream. Secondly, the modified image was encrypted again by permutation matrix.

In 2010, Ismail et al. [58] proposed an image encryption scheme where an external secret key of 104 bit and two chaotic logistic maps were employed to confuse the relationship between the cipher image and the plain image of each pixel of the plain image. The robustness of the system was further reinforced by a feedback mechanism, which made the encryption of each plain pixel depends on the key, the value of the previous cipher pixel and the output of the logistic map (data dependent property). Experimental results demonstrated that the proposed image encryption technique have several interesting features, such as a high level of security, large enough key space, and pixel distributing uniformity. The key stream generator is the key design issue of an encryption system. It directly determines security and efficiency, but most

of the proposed key streams are binary valued, and suffer from short period and limited key space.

Faraoun et al. [59] proposed an n-ary key stream generator, based on hierarchical combination of three chaotic maps and Yoon et al. [60] proposed a new image encryption algorithm with a large pseudorandom permutation which is computed from chaotic maps combinatorially. Since a pseudorandom sequence is securely extended by the permutation matrix, this encryption algorithm shows secure statistical information with relatively short pseudorandom sequences compared to other encryption algorithms. Therefore, the initial conditions or parameters of chaos maps can be chosen with inexpensive cost unlike other chaos-based encryption schemes since the randomness properties of chaotic maps can be effectively spread into encrypted images by using the permutation matrix.

In 2011, Wang et al. [61] proposed a fast image encryption algorithm by combination of permutation and diffusion. In 2013, Sethi et al. [62] proposed a encryption scheme with two phases. In the first phase, the input image is transformed using a new transformation technique, whereas in the second phase, Chirikov standard map is used for pixel shuffling and modified logistic map is used for diffusion. Chirikov standard map, decorrelate the strong relationship among adjacent pixels hence employed to shuffle the pixel positions of the plain image. The modified logistic map is used for generating the random sequence which is completed the purpose of changing pixel values. In 2013, Norouzi et al. [63] proposed a novel algorithm for image encryption based on the hyper-chaotic system. In order to generate the initial conditions of the hyper-chaotic system, 256-bit long external secret key was used. The algorithm consists of three main sections. In the first section, instead of encrypting each pixel, the rows and columns of the image are encrypted using a row-column algorithm. In order to enhance sensitivity, complexity and security, the second section employs masking process which is applied to each quarter of the image (i.e. sub-images) that is to be encrypted, using that sub-image data itself and one of the other sub-images and the average data of other quarters of image. Finally, in the last diffusion section, the four most significant bit planes were encrypted. Experimental results and performance analysis demonstrate the viability of this cryptography based on privacy, integrity and authenticity.

In 2014, Khanzadi et al. [64] proposed an algorithm for image encryption using the random bit sequence generator based on chaotic maps, where chaotic logistic and tent maps are used to generate required random bit sequences. Image encryption schemes

based on chaos usually involve real number arithmetic operations to generate the chaotic orbits from the chaotic system. These operations are time-consuming and are normally performed with high-end processors. To overcome this drawback, in 2014, Fouda et al. [65] proposed a one round encryption scheme for the fast generation of large permutation and diffusion keys based on the sorting of the solutions of the Linear Diophantine Equation (LDE) whose coefficients are integers and dynamically generated from any type of chaotic systems.

In 1994, Adleman [66] released "Molecular Computation of Solutions to Combinatorial Problems" in science, which indicated a new research field-DNA computing. Recent research has considered DNA as a medium for ultra-scale computation and for ultra-compact information storage. With one potential key application being DNA-based, molecular cryptography systems [67]. DNA cryptography is a technique in which DNA is used as an information carrier. The vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are used in cryptography [6].

In 2009, Wang et al. [68] proposed a multilevel image encryption algorithm based on chaos and DNA coding. Here, the location of pixels and pixel values were changed through the combination of chaos with DNA coding. First of all, the digital image was transformed into DNA coding matrix based on DNA code rules. Secondly, this matrix was divided into four sub-matrixes, and disorder these sub-matrixes through logistic chaotic sequence. Then, the sub-matrixes were scrambled by adding new logistic chaotic sequences to get the new sub matrixes. Finally, all scrambled DNA sub-matrixes were joined in a DNA sequence and the scramble DNA matrix was decoded to image matrix. This scheme was effective, and has wide secret key space, strong sensibility, high security with good ability of resisting statistic attack.

Zhang et al. [69] proposed a new image encryption scheme based on XOR operation, bit shift, and DNA sequence addition operation and chaos. The scheme not only could achieve good encryption, but was also resist to exhaustive attack, statistical attack and differential attack. Further in 2012, Zhang et al. [70] proposed a novel image encryption algorithm based on DNA subsequence operation. Different from the traditional DNA encryption methods, this algorithm did not use complex biological operation but used the idea of DNA subsequence operations (such as elongation operation, truncation operation, deletion operation, etc.) combined with the logistic chaotic map to scramble the location and the value of pixel points from the image. The experimental results and security analysis showed superior performance in terms

of encryption effect, has a wide secret key's space, strong sensitivity to secret key, and the abilities of resisting exhaustive attack and statistical attack.

In 2012, Wei et al. [71] used the chaotic sequences generated by Chen's hyper-chaotic map to implement permutation and diffusion from DNA sequence matrices, in which Hamming distance was computed with plain image. In 2012, Liu et al. [72] adopted the PWLCM system for their simplicity in representation. However, because the position index require more time to compute, the processing by pixel increase the computation complexity. In 2014, Huang et al. [73] proposed a new image encryption algorithm based on a four dimensional chaotic map and DNA technology, to perform the permutation by circular avoiding index. Following this, block diffusion operations are adopted to reduce the complexity of the algorithm. Experimental results show a high efficiency for the algorithm.

In 2013, Som et al. [74] proposed a chaos based symmetric key encryption of RGB color images with DNA coding and a chaos based pseudorandom binary number generator (PRBNG). In this algorithm, the plain image was first scrambled using generalized Arnold Cat Map to achieve confusion. The scrambled image pixel were converted to DNA codes and again reconverted to integers where the choice of DNA coding rule was made pseudorandom based on the binary sequences generated by chaos based pseudorandom binary number generator. The integers thus obtained were diffused by performing exclusive OR operation with the integer sequences generated by 1D logistic map producing the cipher image. Currently, many of the methods for data encryption are based on DNA computing.

In 2013, Babaei [75] proposed a reliable data encryption algorithm (OTP) which was stated to be unbreakable, but suffers from some disadvantages. The drawbacks have prevented the common use of its scheme in modern cryptosystems. In this work, a logistic chaotic map has been included as an input of OTP algorithm. So, the obtained simulation result demonstrate the efficiency of proposed algorithm in image encryption. In addition to the cryptography of text files, an interesting encryption algorithm based on a chaotic selection between original message DNA strands and OTP DNA strands has been proposed in this thesis.

Many image encryption schemes have been proposed to protect valuable data from undesirable users. These schemes can be classified into three types: position permutation, gray-value transformation and combination form of first two types. Since position permutation is a simple and effective way to protect a plain image, many scrambling methods such as the algebra-based transformation [8] and chaos-based

transformation [9–11] have been developed to achieve such purpose. However, the algebra-based transformations are fixed and their permutation results are independent of secret key, while most of chaos-based transformations are periodic, linear and consisting of small key space. From a cryptographic point of view, the independence of secret key, the fixed or period transformation and the affine linearity are harmful to security. In 2008, Wang et al. [7] presented a scrambling method based on Poker shuffle technique, in which the shuffle process was controlled by chaotic map. Their method belongs to the position permutation and has several features: nonlinearity, non-analytic formula and can deal with non-square images.

Information hiding techniques [76] have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorised copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence.

Secured message transactions are very much desirable for electronic communications in many ways. In 2010, Jabiullah et al. [77] designed, developed and implemented a secured message transaction technique using Java programming language. For this, a symmetric key encryption technique dynamic Hill cipher has been used for message encryption-decryption with a dynamic key length. A square-matrix of the given key length has been generated with the property that modulo operation of the product of the matrix and the inverse of that matrix is identity. The intended message is converted into binary form, bitwise-XOR operation of the equal two halves of the binary form is performed,and is the operations repeated 3 times to generate the message digest (MD), and concatenate with the message. Encryption is done using the Hill cipher technique with the key matrix and then sent them to the destination. In the receiving end, the reverse process is performed to retrieve the message in secured manner.

The era of "electronic mail" must ensure that two important properties of the "paper mail" system are preserved: (a) messages are private, and (b) messages can be signed. This was demonstrated in [78]. At the heart of proposal was a new encryption method. This method provides an implementation of a "public-key cryptosystem".

A hybrid encryption scheme using public-key encryption to derive a shared key which is then used to encrypt the actual messages using symmetric key techniques.

In 2004, Kurosawa et al. [79] uses a Key Encapsulation Mechanism (KEM) similar to functionality of public key encryption scheme, except the encryption algorithm takes no input other than the recipient's public key. The encryption algorithm is only used to generate and encrypt a key for a symmetric key encryption scheme.

To overcome security and privacy issues [12, 13, 80], fusion of cryptography and biometrics [81] offers a good security feature to protect biometrics during communication and transmission. In 2008, Jain et al. [12] presents a high-level categorization of various vulnerabilities of a biometric system and discuss countermeasures that have been proposed to address these vulnerabilities.

Biometric template protection is one of the most important issues in deploying a practical biometric system. To tackle this problem, many algorithms, that do not store the template in its original form, have been reported in recent years. They can be categorized into two approaches, namely biometric cryptosystem and transform-based. However, most (if not all) algorithms in both approaches offer a trade-off between the template security and matching performance. Moreover, it is believed that no single template protection method is capable of satisfying the security and performance simultaneously. In 2010, Feng et al. [82] presented a hybrid approach which takes advantage of both the biometric cryptosystem approach and the transform-based approach. A three-step hybrid algorithm is designed and developed based on Random Projection, Discriminability-Preserving (DP) transform, and Fuzzy Commitment scheme. The proposed algorithm not only provides good security, but also enhances the performance through the DP transform.

Multibiometric systems are being increasingly deployed in many large-scale biometric applications (e.g., FBI-IAFIS, UIDAI system in India) because of their advantages of lower error rates and larger population coverage compared to unibiometric systems. However, multibiometric systems require storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user, which results in increased risk to user privacy and system security. In 2012, Nagar et al. [83] proposed a feature-level fusion framework to simultaneously protect multiple templates of a user as a single secure sketch. The main contribution includes practical implementation of the proposed feature-level fusion framework using two well-known biometric cryptosystems, namely, fuzzy vault and fuzzy commitment. Experimental results show that both the multibiometric cryptosystems have higher security and matching performance compared to their unibiometric counterparts.

In 2014, Cheepchol et al. [84] presents the digital image encryption scheme for

biometric facial image using Cellular Automata (CA) for secure image storage. This scheme is relatively simple using a segmentation of CA binary image with embedded secret keys generated by the third class of well-known Wolfram Cellular Automata that exhibits chaotic patterns. Such segmented CA binary image are diffused to the shuffled and bitplane separated of the original biometric facial image through XOR operations. Imaging security and biometrics are two heavily connected areas. Quick evolution of biometrics has raised the need of securing biometric data. A majority of this data is visual, which has lead to intensive development of image security techniques for biometric applications. In 2012, Marques et al. [85] reviews a fast fly over image security approaches and imaging-related biometrics.

Fingerprint recognition is one of the most popular and successful methods used for person identification, which takes advantage of the fact that the fingerprint has unique characteristics called minutiae; which are the points where a curve track finishes, intersect with other track or branches off. In 2009, Leon et al. [86] proposed a novel method for fingerprint recognition using a combination of Fast Fourier Transform (FFT) and Gabor Filters to enhancement the fingerprint image.

In 2010, Kaur et al. [14] developed a system to encrypt and decrypt the biometric image using helper data of a fingerprint and password to make it secure so that even if someone gains access to the encrypted image stored in the database original image cannot be reproduced from it. Again in 2012, Bhowmik et al. [87] proposed steps to represent a complete process of fingerprint feature extraction for minutiae matching. Over the past years, several different approaches have been proposed for extracting distinguishable features and improving classification performance. In 2010, Rajanna et al. [88] presents a comparative study involving four different feature extraction methods for fingerprint classification and proposed a rank-based fusion scheme for improving classification performance. Among all the biometrics, fingerprints are the oldest and very widely used in personal verification systems. This provides a strong motivation for developing techniques that can protect the biometrics fingerprint data particularly during communication and transmission over insecure network channels.

In 2012, Bhatnagar et al. [89] proposed a security solution during communication and transmission of fingerprint data in the form of a novel encryption technique based on Fractional Random Wavelet Transform (FrRnWT). Again in 2014, Bhatnagar et al. [90] proposed a security solution during communication and transmission of fingerprint data in the form of a novel encryption technique based on Reversible Hidden Transform (RHT) and Fractional Wavelet Packet Transform (FrWPT). These

security solutions relies on both spatial and frequency domains. In another work Bhatnagar et al. [91] proposed framework based on the Fractional Wavelet Packet Transform (FrWPT), chaotic map and Hessenberg decomposition. The core idea is to shuffle biometrics image using affine transform followed by the transformation in FrWPT domain with chaotically generated transform orders. Now, FrWPT coefficients are altered using the Hessenberg decomposition. One main challenge of cryptographic systems processes to protect private keys from attackers. A fuzzy vault refers to a biometric cryptosystem that has been used to effectively protect private keys. In biometric systems, a critical problem is storing biometric templates in a database. However, fuzzy vault systems do not need to directly store these templates since they are combined with private keys by using cryptography.

In 2013, Bringer et al. [92] proposed techniques to secure two-party computation (also known as secure function evaluation) to biometric identification. These techniques enable to compute biometric identification algorithms such as homomorphic encryption, Garbled Circuits (GCs), and Oblivious Transfers (OTs) while maintaining the privacy of the biometric data. In recent years, a variety of encryption algorithms were proposed to enhance the security of software and systems. Validating whether encryption algorithms are correctly implemented is a challenging issue. Software testing delivers an effective and practical solution, but it also faces the oracle problem (that is, under many practical situations, it is impossible or too computationally expensive to know whether the output for any given input is correct). In 2014, Sun et al. [93] proposed a property-based approach to testing encryption programs in the absence of oracles. Experimental results show that even without oracles, the proposed approach could detect nearly 50% inserted faults.

1.7 Motivation

Hill cipher has been a candidate algorithm for data encryption due to its resistant to the frequency letter analysis. It is very simple since, it uses matrix multiplication. It can be implemented with high speed operation leading high throughput. However, Hill cipher can be broken with a known plaintext attack revealing weak security. It requires inverse of the key matrix in decryption. Moreover, Hill cipher algorithm cannot encrypt images that contain large areas of a single colour or gray level. This motivated to repair the flaws of Hill cipher and to propose encryption schemes to encrypt images with homogeneous background. Two important attributes of a powerful encryption

technique are diffusion and confusion. Hence, the motivation is to generate a scheme which has more diffusion and confusion.

Due to some intrinsic features of images, some of the traditional encryption schemes are not very suitable for image encryption. Hence the motivation is to generate schemes to encrypt images efficiently.

In particular, the objectives of the thesis are to:

- generate invertible, involutory and permutation key matrices.
- develop schemes to encrypt image efficiently.
- develop schemes which take less encryption and decryption time.
- Generate schemes which maintain good NPCR, UACI, MAE, PSNR and entropy value, and have more diffusion and confusion leading to difficult in cryptanalysis.
- develop schemes which protect the images maintaining close to zero correlation coefficient between adjacent pixels of encrypted images.
- develop schemes to encrypt biometric images so as to enhance the transmission security.

1.8 Thesis Layout

Following this chapter on introduction this thesis consists of 6 chapters. The rest of the thesis is organized as follows:

Chapter 2- Generation of New Hill Cipher Key Matrices: Applications to Encryption of Conventional and Biometric Image:

In this chapter, novel methods of generating invertible, involutory and permutation key matrix generation for Hill cipher have been proposed. Invertible, involutory matrix generation method solves the key matrix inversion problem. Permutation key matrix generation method increases the Hill system's security considerably. Involutory matrix, eliminates necessity of matrix inverse for Hill decryption. This means that same machinery can be used both for encryption and decryption of massages; no additional hardware is required to compute inverse before decrypting. Advanced

Hill cipher algorithm and H-S-X cryptosystem proposed in this chapter and these have been applied to encrypt conventional and biometric images. The corresponding FPGA implementation has been presented. In advanced Hill cipher algorithm FPGA implementation with three different types of multipliers such as conventional array multiplier, Booth-Wallace multiplier and Vedic multiplier method have been employed. A comparative study with implemented methods in terms of number of multipliers, adders and slices used as well as maximum combinational path delay and power consumption has been carried out and the results are presented.

Chapter 3- Conventional and Biometric Image Encryption by Using Extended Hill Cipher Algorithm:

Shastry et al. [50,52] have proposed modified Hill cipher algorithms for text encryption. The first one is based on interweaving and iteration, where as second one is based on key dependent permutation and circular rotation. In this chapter these two schemes have been applied for image encryption. Further, an extended Hill cipher algorithm based on XOR and zigzag operation for image encryption has been proposed. It is observed that the key dependent permutation and circular rotation is lossy in nature, where as interweaving and iteration is a loss less one. The proposed extended Hill cipher algorithm has been applied for encryption of both conventional and biometric images. Simulation experiments are carried out on standard images using all the three approaches. The results revealed that the proposed extended Hill cipher algorithm offers the lower encryption and decryption time compared to other two methods. The hybrid cryptosystem which is the combination of extended Hill cipher technique and RSA algorithm has been implemented to solve the key distribution problem and to enhance the security with reduced encryption and decryption time.

Chapter 4- Development of Novel Multilevel Image Encryption Scheme:

This chapter deals with multilevel image encryption schemes by combining ideas related to chaos based DNA coding [68] along with shifting and scrambling or poker shuffle [7] strategy. In the DNA based methods, DNA is used as an information carrier and the recent biological technique used as an implementation tool. In this chapter, two distinct approaches for image encryption has been suggested. In the

first approach, results obtained from chaos based DNA coding scheme is shifted and scrambled to produce the final result. On the other hand in the second approach the results obtained from chaos based DNA coding encryption is followed by poker shuffle operation to generate the final result. These two methods have been simulated for encryption and decryption of image and the results obtained have been compared and discussed. Subsequently, FPGA implementation of proposed cryptosystem has been carried out.

Chapter 5- Development of a Secured Image Transaction and Authentication Scheme:

In this chapter a modified Hill cipher is proposed which is the combination of three techniques. This proposed modified Hill cipher takes advantage of all the three techniques. The encryption methods proposed in chapters 2, 3 and 4 provides only confidentiality of information by encryption. Recent applications demand authenticity, integrity and non-repudiation of the information in addition to confidentiality. Keeping this requirement in mind a novel hybrid method has been implemented. This method has employed proposed modified Hill cipher to provide confidentiality. Produced message digest encrypted by private key of RSA algorithm to achieve other features such as authenticity, integrity, and non-repudiation.

Chapter 6- Secure Image Encryption Using Fingerprint and Password:

Fusion of cryptography and biometric provides enhanced security. In this chapter, a biometric cryptosystem approach that combines cryptography and biometrics has been proposed. Under this approach, the image is encrypted with the help of fingerprint and password. A key generated with the combination of fingerprint and password and is used for image encryption. This mechanism is seen to enhance the security of biometrics images during transmission. The proposed method has been validated using simulation studies.

Chapter 7- Conclusion and Future Work:

This chapter provides the concluding remarks with a stress on achievements and limitations of the present work. The scopes for further research are outlined at the

end.

The contributions made in each chapter are discussed in sequel, which include proposed schemes, their simulation results, security analysis and the comparative analysis.

Chapter 2

Generation of New Hill Cipher Key Matrices: Applications to Encryption of Conventional and Biometric Image

Chapter 2

Generation of New Hill Cipher Key Matrices: Applications to Encryption of Conventional and Biometric Image

Hill cipher is one of the most famous symmetric cryptosystem that is used to protect information from unauthorized access. Hill cipher has many advantages in data encryption. First, it is resistant to the frequency letter analysis. It's also very simple since it uses matrix multiplication. Finally, it has high speed and high throughput. Hill cipher requires inverse of the key matrix during decryption. In fact, that not all the matrices have an inverse and therefore they will not be eligible as key matrices in the Hill cipher scheme. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. Moreover, Hill cipher algorithm cannot encrypt images that contain large areas of a single colour or gray level. Thus, it does not hide all features of the image which reveals patterns in the plaintext. In order to repair these flaws of the Hill cipher, different schemes have been proposed [19–23].

In this chapter, novel methods of generating invertible, involutory and permutation key matrix generation methods for Hill cipher has been proposed. Invertible, involutory matrix generation method solves the key matrix inversion problem. Permutation key matrix generation method enhancement increases the Hill system's security considerably. Involutory matrix, which eliminates necessity of matrix inverse for Hill decryption. This meant that same machinery could be used both for

encryption and decryption of massages; no additional hardware would be needed to compute inverses before decrypting. Moreover the algorithm can generate the different key matrix for each block encryption instead of keeping the key matrix constant. This increases the secrecy of data. Finally, in this chapter, involutory key matrix generation method applied to encrypt conventional and biometric image using advanced Hill cipher algorithm and H-S-X cryptosystem and its FPGA implementation has been done. In advanced Hill cipher algorithm FPGA implementation performed by using three methods which are conventional array multiplier, Booth Wallace multiplier and Vedic multiplier. Also comparison has been made with implemented methods in respect to number of multipliers and adders used, number of slices used, maximum combinational path delay and power consumption.

The remaining chapter is organized as follows. In Section 2.1, the basic concept of Hill cipher is explained. In Section 2.2, proposed algorithms for invertible matrix generation method is presented. Section 2.3 consists of proposed algorithms for involutory matrix generation where as the proposed algorithm for permutation matrix generation is outlined in Section 2.4. Section 2.5 presents image encryption using proposed advanced Hill cipher algorithm and its FPGA implementation. In Section 2.6, FPGA implementation of proposed H-S-X cryptosystem for image encryption is outlined. Finally, a summary of the chapter is presented in Section 2.7.

2.1 Hill Cipher

Hill cipher is an application of linear algebra to cryptology [15, 16]. It was developed by the mathematician Lester S. Hill. The Hill cipher algorithm takes m successive plaintext letters and substitutes them by m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value ($a = 0, b = 1, ..., z = 25$). Let m be a positive integer, the idea is to have m linear combinations of the m alphabetic characters in one plaintext element and produce corresponding m characters in one ciphertext element. Then, a $m \times m$ matrix A is used as a key of the system such that A is invertible modulo 26.

Let a_{ij} be the entry of A. For the plaintext block $x = (x_1, x_2, ..., x_m)$ (the numerical equivalents of m letters) and a key matrix A, the corresponding ciphertext block $y = (y_1, y_2, ..., y_m)$ can be computed as follows:

Encryption: The ciphertext can be computed by

$$(y_1, y_2, ..., y_m) = (x_1, x_2, ..., x_m)A(\text{mod}26) \tag{2.1}$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1m} \\ a_{21} & a_{22} & ... & a_{2m} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mm} \end{bmatrix}$$

The ciphertext is obtained from the plaintext by means of a linear transformation.

Decryption: The reverse process, deciphering, is computed by

$$(x_1, x_2, ..., x_m) = (y_1, y_2, ..., y_m)A^{-1}(\text{mod}26). \tag{2.2}$$

where

$$A^{-1} = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1m} \\ a_{21} & a_{22} & ... & a_{2m} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mm} \end{bmatrix}^{-1} (\text{mod}26)$$

Since the block length is m, there are $26m$ different m letters blocks possible, each of which can be regarded as a letter in a $26m$ letter combination. Hill's method amounts to a mono-alphabetic substitution on this alphabet [58, 94].

2.2 Proposed Algorithms for Invertible Matrix Generation

The matrix generated in invertible matrix formulation scheme is always invertible to be used as a key matrix in Hill cipher scheme. Here we have proposed two invertible matrix formulation methods.

Algorithm 1:

1. Select a random matrix A of size $m \times m$.

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1m} \\ a_{21} & a_{22} & ... & a_{2m} \\ . & . & . & . \\ a_{m1} & a_{m2} & ... & a_{mm} \end{bmatrix} \tag{2.3}$$

2. If it is singular and of rank $m-1$, then select A_{ii} = principal minor by eliminating i^{th} row and i^{th} column of A, such that ΔA_{ii} is non-zero.

3. Then add 1 to the diagonal element which is not included in non-singular, i.e.

$$a_{ii} \leftarrow a_{ii} + 1 \tag{2.4}$$

4. To generate the above method: If the rank of A is l, select non-singular principal-minor $(l \times l)$.

5. Then add 1 to all the principal diagonal elements which are not included in the principal-minor.

Above method has one limitation as to determine the rank of the matrix.

Algorithm 2:

1. Select a matrix A of size $m \times n$

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ . & . & . & . \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix} \tag{2.5}$$

where

a_{11} = seed number (generation of random number)

$a_{12} = (a_{11} \times t) \bmod n$, where t is any number prime to n.

$a_{13} = (a_{12} \times t) \bmod n$

$\vdots$

$a_{21} = (a_{1n} \times t) \bmod n$

$\vdots$

$a_{mn} = (a_{m(n-1)} \times t) \bmod n$

2. Such matrix A has rank one, if Trace A mod $n \neq 0$, then $K = A + I$, provided that the eigen value of A is not equal to $(n-1)$.

3. K can be found by adding 1 to any $(m-1)$ diagonal elements.

4. And if Trace A mod $n = 0$, then $K = A + aI$, where a is any scalar. Since the inversion of higher dimensional matrix is time consuming, another method of encryption by introducing involutory K matrix, where
$K = K^{-1}$ or $K^2 = I$.

2.3 Proposed Algorithms for Involutory Matrix Generation

2.3.1 Generation of Involutory 2×2 Matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ then $A^{-1} = \frac{\text{adjoint}(A)}{\text{determinant}(A)} = \frac{(\text{cofactor}(A))^T}{\text{determinant}(A)}$

therefore $A^{-1} = \frac{1}{\Delta a} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$ where Δa is the determinant(A).

A is said to be involutory, if $A = A^{-1}$
So, $a_{12} = -a_{12}/\Delta a$ and $a_{21} = -a_{21}/\Delta a$
therefore $\Delta a = -1$ and $a_{11} = -a_{22} \Rightarrow a_{11} + a_{22} = 0$.
(since $a_{11} = \frac{a_{22}}{\Delta a}$ and $a_{22} = \frac{a_{11}}{\Delta a}$ and $\Delta a = -1$)

Example:(For modulo 13)

$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ -5 & -4 \end{bmatrix}$
$\Delta a = -1$
$a_{11} + a_{22} = 4 - 4 = 0$
$a_{11} = \frac{a_{22}}{\Delta a} = \frac{-4}{-1} = 4$
$a_{21} = \frac{-a_{21}}{\Delta a} = \frac{5}{-1} = -5$
Therefore, A is an involutary matrix.

2.3.2 Generation of Involutory 3×3 matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$

where $A_{11} = [a_{11}]$ is a 1×1 matrix, $A_{12} = [a_{12} \;\; a_{13}]$ is a 1×2 matrix,

$A_{21} = \begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}$ is a 2×1 matrix and $A_{22} = \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix}$ is a 2×2 matrix.

If A is involutory then

$A_{11}^2 + A_{12}A_{21} = I, A_{11}A_{12} + A_{12}A_{22} = 0,$

$A_{21}A_{11} + A_{22}A_{21} = 0$, and $A_{21}A_{12} + A_{22}^2 = I$

Since $A_{11} = [a_{11}]$ is 1×1 matrix and $A_{21}(a_{11}I + A_{22}) = 0$, so for non-trivial solution, it is necessary that $a_{11}I + A_{22} = 0$, i.e. $a_{11} = -$(one of the eigenvalues of A_{22}).

$A_{21}A_{12}$ can also be written as

$$A_{21}A_{12} = \begin{bmatrix} a_{21} & 0 \\ a_{31} & 0 \end{bmatrix} \begin{bmatrix} a_{12} & a_{13} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{21}a_{12} & a_{21}a_{13} \\ a_{31}a_{12} & a_{31}a_{13} \end{bmatrix}$$

So $A_{21}A_{12}$ is singular and $A_{21}A_{12} = I - A_{22}^2$.

Hence, A_{22} must have an eigenvalue ± 1.

It can be shown that $Trace\,[A_{21}A_{12}] = A_{12}A_{21}$.

Since, it can be proved that if $A_{11} = a_{11} = -$(one of the eigenvalues of A_{22}), then any non-trivial solution of $A_{21}A_{12} = I - A_{22}^2$ will also satisfy $A_{12}A_{21} = 1 - a_{11}^2$.

Example: (For modulo 13)

Consider $A_{22} = \begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix}$ which has eigenvalues $\lambda = 1$ and 7.

$a_{11} = -7 = 6$ or $-1 = 12$. If $a_{11} = 6$, then,

$$A_{21}A_{12} = I - A_{22}^2 = I - \begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix} = I - \begin{bmatrix} 9 & 1 \\ 8 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 5 & 12 \end{bmatrix}$$

$a_{21}a_{12} = 5$. So, $a_{21} = 5$ and $a_{12} = 1$.

$a_{21}a_{13} = 12$. So, $a_{13} = \frac{12}{5} = 5$ and $a_{31} = \frac{5}{1} = 5$.

So the matrix will be $A = \begin{bmatrix} 6 & 1 & 5 \\ 5 & 2 & 5 \\ 5 & 1 & 6 \end{bmatrix}$.

Other matrix can also be obtained by considering $a_{11} = 12$.

2.3.3 Generation of Involutory 4×4 Matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$

be an involutory matrix partitioned as, $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ where

$A_{11} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, A_{12} = \begin{bmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{bmatrix}, A_{21} = \begin{bmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix}, A_{22} = \begin{bmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{bmatrix}.$

Then, $A_{12}A_{21} = I - A_{11}^2, A_{11}A_{12} + A_{12}A_{22} = 0,$

$A_{21}A_{11} + A_{22}A_{21} = 0$, and $A_{21}A_{12} = I - A_{22}^2$.

In order to obtain solution for all the four matrix equations, $A_{12}A_{21}$ can be factorized as $A_{12}A_{21} = (I - A_{11})(I + A_{11})$

So, if $A_{12} = (I - A_{11})k$ or $(I + A_{11})k$, then

$A_{21} = (I + A_{11})\frac{1}{k}$ or $(I - A_{11})\frac{1}{k}$, where k is a scalar constant.

Then, $A_{11}A_{12} + A_{12}A_{22} = A_{11}(I - A_{11})k + (I - A_{11})kA_{22} = k(A_{11} + A_{22})(I - A_{11})$.

So, $A_{11} + A_{22} = 0$ or $A_{11} = I$.

Since $A_{11} = I$ is a trivial solution, then $A_{11} + A_{22} = 0$ is taken.

When we solve the 3^{rd} and 4^{th} matrix equations, same solution is obtained.

Example: (For Modulo 13)

Consider $A_{22} = \begin{bmatrix} 1 & 3 \\ 8 & 4 \end{bmatrix}$ then $A_{11} = \begin{bmatrix} 12 & 10 \\ 5 & 9 \end{bmatrix}$.

Since, $A_{11} + A_{22} = 0$. Therefore, $A_{11} = -A_{22}$.

Consider $A_{12} = (I - A_{11})k$ with $k = 1$. Then $A_{12} = \begin{bmatrix} 2 & 3 \\ 8 & 5 \end{bmatrix}$.

Similarly, take $A_{21} = (I + A_{11})\frac{1}{k}$ with $k = 1$. Then, $A_{21} = \begin{bmatrix} 0 & 10 \\ 5 & 10 \end{bmatrix}$.

Hence, $A = \begin{bmatrix} 12 & 10 & 2 & 3 \\ 5 & 9 & 8 & 5 \\ 0 & 10 & 1 & 3 \\ 5 & 10 & 8 & 4 \end{bmatrix}$

2.3.4 A General Method of Generating an Even Involutory Matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{bmatrix}$ be an $n \times n$ involutory matrix partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, where n is even and $A_{11}, A_{12,}A_{21}$ and A_{22} are matrices of order $\frac{n}{2} \times \frac{n}{2}$ each.

So, $A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$.

If A_{12} is one of the factors of $I - A_{11}^2$ then A_{21} is the other.

Solving the 2^{nd} matrix equation, results $A_{11} + A_{22} = 0$. Then form the matrix.

Algorithm:

1. Select any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix A_{22}.
2. Obtain $A_{11} = -A_{22}$.
3. Take $A_{12} = k(I - A_{11})$ or $k(I + A_{11})$ for k, a scalar constant.
4. Then, $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$.
5. Form the complete matrix A.

Example: (For Modulo 13)

Let $A_{22} = \begin{bmatrix} 10 & 2 \\ 3 & 4 \end{bmatrix}$, then $A_{11} = \begin{bmatrix} 3 & 11 \\ 10 & 9 \end{bmatrix}$.

If k is selected as 2, then $A_{12} = k(I - A_{11}) = \begin{bmatrix} 9 & 4 \\ 6 & 10 \end{bmatrix}$

and $A_{21} = \frac{1}{k}(I + A_{11}) = \begin{bmatrix} 2 & 12 \\ 5 & 5 \end{bmatrix}$.

So, $A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}$.

2.3.5 A General Method of Generating an Involutory Matrix

Let $A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{bmatrix}$ be an $n \times n$ involutory matrix partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ where,

$A_{11} = [a_{11}]$ is a 1×1 matrix,

$A_{12} = \begin{bmatrix} a_{12} & a_{13} & ... & a_{1n} \end{bmatrix}$ is a $1 \times (n-1)$ matrix,

$A_{21} = \begin{bmatrix} a_{21} \\ a_{31} \\ ... \\ a_{n1} \end{bmatrix}$ is a $(n-1) \times 1$ matrix and

$A_{22} = \begin{bmatrix} a_{22} & a_{23} & ... & a_{2n} \\ a_{32} & a_{33} & ... & a_{3n} \\ ... & ... & ... & ... \\ a_{n2} & a_{n3} & ... & a_{nn} \end{bmatrix}$ is a $(n-1) \times (n-1)$ matrix.

So,

$$A_{12}A_{21} = I - A_{11}^2 = 1 - a_{11}^2 \tag{2.6}$$

and $A_{12}(a_{11}I + A_{22}) = 0$.

Also, a_{11}=-(one of the eigenvalues of A_{22} other than 1).

Since $A_{21}A_{12}$ is a singular matrix having the rank 1 and

$$A_{21}A_{12} = I - A_{22}^2 \tag{2.7}$$

So, A_{22}^2 must have rank of $(n-2)$ with eigenvalues $+1$ of $(n-2)$ multiplicity.

Therefore, A_{22} must have eigenvalues ± 1.

It can also be shown that the consistent solution obtained for elements A_{21} and A_{12} by solving the equation (2.7) term by term will also satisfy the equation (2.6).

Algorithm:

1. Select A_{22}, a non-singular $(n-1) \times (n-1)$ matrix, which has $(n-2)$ number of eigenvalues and which are either ± 1 or both.

2. Determine the other eigenvalue λ of A_{22}.

3. Set $a_{11} = -\lambda$.

4. Obtain the consistent solution of all elements of A_{21} and A_{12} by using (2.7).

5. Formulate the matrix.

Example: (For modulo 13)

Let $A_{22} = \begin{bmatrix} 9 & 6 & 10 \\ 12 & 10 & 2 \\ 5 & 3 & 4 \end{bmatrix}$ which has eigenvalues $\lambda = \pm 1, 10$.

So, $A_{11} = [3]$, and one of the consistent solutions of $A_{12} = \begin{bmatrix} 11 & 9 & 4 \end{bmatrix}$ and $A_{21} = \begin{bmatrix} 10 \\ 2 \\ 5 \end{bmatrix}$.

So, $A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}$.

Another consistent solution of $A_{12} = \begin{bmatrix} 1 & 2 & 11 \end{bmatrix}$ and $A_{21} = \begin{bmatrix} 6 \\ 9 \\ 3 \end{bmatrix}$.

So, $A = \begin{bmatrix} 3 & 1 & 2 & 11 \\ 6 & 9 & 6 & 10 \\ 9 & 12 & 10 & 2 \\ 3 & 5 & 3 & 4 \end{bmatrix}$.

2.3.6 Another Method to Generate Involutory Matrix

Let A be any non-singular matrix and E be its eigen matrix. Then we know that $AE = E\lambda$, where λ is diagonal matrix with the eigenvalues as diagonal elements. E the eigen matrix is non-singular.

Then, $A = E\lambda E^{-1}$ and $A^{-1} = (E\lambda E^{-1})^{-1} = E^{-1}\lambda^{-1}E = E\lambda^{-1}E^{-1}$.

So, $A = A^{-1}$ only when $\lambda = \lambda^{-1}$.

If $\lambda = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 & . & . & 0 \\ 0 & \lambda_2 & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & \lambda_n \end{bmatrix}$ then, $\lambda^{-1} = \begin{bmatrix} \frac{1}{\lambda_1} & 0 & 0 & . & . & . & 0 \\ 0 & \frac{1}{\lambda_2} & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & \frac{1}{\lambda_n} \end{bmatrix}$.

Thus $\lambda = \lambda^{-1}$ when $\lambda_i = \frac{1}{\lambda_i}$ or $\lambda_i = \pm 1$.

Algorithm:

1. Select any non-singular matrix E.
2. Form a diagonal matrix λ with $\lambda = \pm 1$ but all value of λ must not be equal.
3. Then compute $E\lambda E^{-1} = A$.

Example: (For modulo 13)

$$\text{Let } E = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 8 \end{bmatrix} \Rightarrow E^{-1} = \begin{bmatrix} -\frac{8}{3} & \frac{8}{3} & -1 \\ \frac{10}{3} & \frac{13}{3} & 2 \\ -1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} 6 & 7 & 12 \\ 12 & 0 & 2 \\ 12 & 2 & 12 \end{bmatrix}$$

$$\text{Take } \lambda = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$\text{So, } A = E\lambda E^{-1} = \begin{bmatrix} 1 & 11 & 3 \\ 4 & 8 & 6 \\ 7 & 5 & 8 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 6 & 7 & 12 \\ 12 & 0 & 2 \\ 12 & 2 & 12 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 5 \\ 10 & 1 & 6 \\ 3 & 0 & 8 \end{bmatrix}.$$

2.3.7 Involutory Matrix Formulation

Method of generating random involutory matrix is described as follows:

$$\text{Let } A = \begin{bmatrix} b & bt & bt^2 ... & bt^{m-1} \\ bt^m & bt^{m+1} & bt^{m+2} ... & bt^{2m-1} \\ ... & ... & ..... & ... \\ bt^{m(m-1)} & bt^{m(m-1)+1} & bt^{m(m-1)+2} ... & bt^{m^2-1} \end{bmatrix} \text{ is a matrix of size } m \times m$$

generated by a set of random number of modulo n given by

$$a_{ij} = bt^{m(i-1)+j-1} \bmod n \tag{2.8}$$

where b is the seed element and multiplying factor t is singular of rank 1 if $traceA \neq 0 \bmod n$ and rank 0 if $traceA = 0 \bmod n$.

Proof: It is proved that if λ_i is the eigenvalue of matrix $A(m \times m)$, then the characteristic equation of A,

$\lambda_i^m + a_{m-1}\lambda_i^{m-1} + ... + a_0 = 0$ for $i = 1, ..., m$

Then, $s_m + a_{m-1}s_{m-1} + ... + a_1 s_1 + na_0 = 0$

where, $s_j = \sum_{i=1}^{n} \lambda_i^{j-1} = trace \text{ of } A^j$

After due algebraic manipulation it can be shown that

$s_1 + a_{m-1} = 0$

$s_2 + s_1 a_{m-1} + 2a_{m-2} = 0$

$s_{m-k} + a_{m-1}s_{m-1} + ... + (m-k)a_K = 0$

...

$s_{m-1} + a_{m-1}s_{m-2} + ... + a_2 s_1 + (m-1)a_1 = 0$

$s_m + a_{m-1}s_{m-1} + ... + ma_0 = 0$

Trace of $A = b[1 + t^{m+1} + t^{2(m+1)} + t^{3(m+1)} + ... + t^{(m-1)(m+1)}] = b.g(t)$

where $g(t) = 1 + t^{m+1} + t^{2(m+1)} + t^{3(m+1)} + ... + t^{(m-1)(m+1)}$

The trace of $A^2 = b^2 g^2(t)$, trace of $A^j = b^j g^j(t)$ and trace of $A^m = b^m g^m(t)$.

So, $a_{m-1} = -s_1 = -g(t) \bmod n$

$a_{m-2} = -\frac{1}{2}[s_2 + a_{m-1}s_1] = -\frac{1}{2}[(g(t))^2 - (g(t))^2] = 0$

$a_{m-3} = -\frac{1}{3}[s_3 + a_{m-1}s_2 + a_{m-2}s_1] = -\frac{1}{3}[(g(t))^3 - g(t)(g(t))^2] = 0$

$a_{m-4} = -\frac{1}{4}[s_4 + a_{m-1}s_3 + a_{m-2}s_2 + a_{m-3}s_1] = -\frac{1}{4}[(g(t))^4 - g(t)(g(t))^3] = 0$

Similarly, $a_1 = 0, a_0 = 0$. So, $\lambda^m - k\lambda^{m-1} = 0$ where, $k = bg(t) \bmod n$.

Hence the matrix has $(m-1)$ number of eigenvalue of zero and one eigenvalue of k.

Formulation of Matrix:

Let $A = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1m} \\ a_{21} & a_{22} & ... & a_{2m} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mm} \end{bmatrix}$ be an $m \times m$ involutory matrix partitioned to $\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ where

$A_{11} = [a_{11}]$ is a 1×1 matrix,

$A_{12} = \begin{bmatrix} a_{12} & a_{13} & ... & a_{1m} \end{bmatrix}$ is a $1 \times (m-1)$ matrix,

$A_{21} = \begin{bmatrix} a_{21} \\ a_{31} \\ ... \\ a_{m1} \end{bmatrix}$ is a $(m-1) \times 1$ matrix, and

$A_{22} = \begin{bmatrix} a_{22} & a_{23} & ... & a_{2m} \\ a_{32} & a_{33} & ... & a_{3m} \\ ... & ... & ... & ... \\ a_{m2} & a_{m3} & ... & a_{mm} \end{bmatrix}$ is a $(m-1) \times (m-1)$ matrix.

If $A_{22} = A + I$, then A_{22} will have eigenvalue 1 of $m-2$ multiplicity and $(m-1)^{th}$

eigenvalue will be $k+1$ where $k =$ trace of A.
So, $a_{11} = -(k+1)$, that is $a_{11} = -$(one of the eigenvalues of A_{22} other than 1) and $A_{21}A_{12} = I - A_{22}^2$ which can have multiple solutions and can be solved.

Algorithm:

1. Form the matrix A , with the seed number b and multiplying factor t
2. Take $A_{22} = A + I$
3. A_{22} will have eigenvalue 1 of $(m-2)$ multiplicity and $(m-1)^{th}$ eigenvalue will be $k+1$ where $k = \ trace\ of\ A$
4. Set $a_{11} = -(k+1)$
5. Obtain the consistent solution of all elements of A_{21} and A_{12} by using the equation $A_{21}A_{12} = I - A_{22}^2$
6. Formulate the complete matrix

Example:1 (For modulo 13)

Consider seed number, $b = 11$ and multiplying factor, $t = 3$. Let B is a 3×3 involutory matrix,
Then

$$A = \begin{bmatrix} b & bt \\ bt^2 & bt^3 \end{bmatrix} \bmod 13$$

$$A = \begin{bmatrix} 11 & 7 \\ 8 & 11 \end{bmatrix}$$

$$A_{22} = A + I = \begin{bmatrix} 11 & 7 \\ 8 & 11 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 12 & 7 \\ 8 & 12 \end{bmatrix}$$

Eigenvalues of $A22$ are $1, 10$.
So,

$$A_{11} = [b_{11}] = [-10] = [3] = 3$$

and

$$A_{21}A_{12} = I - (A_{22})^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 200 & 168 \\ 192 & 200 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 5 & 12 \\ 10 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} -4 & -12 \\ -10 & -4 \end{bmatrix} = \begin{bmatrix} 9 & 1 \\ 3 & 9 \end{bmatrix}$$

$$A_{21}A_{12} = \begin{bmatrix} b_{21} & 0 \\ b_{31} & 0 \end{bmatrix} \begin{bmatrix} b_{12} & b_{13} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} b_{21}b_{12} & b_{21}b_{13} \\ b_{31}b_{12} & b_{31}b_{13} \end{bmatrix}$$

Equating above two equations we have,

$$b_{21}b_{12} = 9, b_{21}b_{13} = 1, b_{31}b_{12} = 3, b_{31}b_{13} = 9$$

If

$$b_{21} = 1, then\ b_{12} = 9, b_{13} = 1, b_{31} = \frac{3}{9} = 9$$

Therefore

$$B = \begin{bmatrix} 3 & 9 & 1 \\ 1 & 12 & 7 \\ 9 & 8 & 12 \end{bmatrix}$$

Example:2 (For modulo 17)

Take seed number, $b = 5$ and multiplying factor, $t = 7$. Let B is a 4×4 involutory matrix, i.e.

$$B = \begin{bmatrix} b_{11} & \vdots & b_{12} & b_{13} & b_{14} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ b_{21} & \vdots & b_{22} & b_{23} & b_{24} \\ b_{31} & \vdots & b_{32} & b_{33} & b_{34} \\ b_{41} & \vdots & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

is partitioned to

$$\begin{bmatrix} A_{11} & \vdots & A_{12} \\ \cdots & \vdots & \cdots \\ A_{21} & \vdots & A_{22} \end{bmatrix}$$

$$A = \begin{bmatrix} b & bt & bt^2 \\ bt^3 & bt^4 & bt^5 \\ bt^6 & bt^7 & bt^8 \end{bmatrix} \text{mod} 17 = \begin{bmatrix} 5 & 1 & 7 \\ 15 & 3 & 4 \\ 11 & 9 & 12 \end{bmatrix}$$

So,

$$A_{22} = A + I = \begin{bmatrix} 6 & 1 & 7 \\ 15 & 4 & 4 \\ 11 & 9 & 13 \end{bmatrix}$$

The eigenvalues of A_{22} are $1, 1, 4$.

Therefore,

$$A_{11} = [b_{11}] = [-4] = [13] = 13 \, and$$

$$A_{21}A_{12} = I - A_{22}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 9 & 5 & 1 \\ 7 & 16 & 3 \\ 4 & 11 & 10 \end{bmatrix} = \begin{bmatrix} 9 & 12 & 16 \\ 10 & 2 & 14 \\ 13 & 6 & 8 \end{bmatrix}$$

$$A_{21}A_{12} = \begin{bmatrix} b_{21} & 0 & 0 \\ b_{31} & 0 & 0 \\ b_{41} & 0 & 0 \end{bmatrix} - \begin{bmatrix} b_{12} & b_{13} & b_{14} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} b_{21}b_{12} & b_{21}b_{13} & b_{21}b_{14} \\ b_{31}b_{12} & b_{31}b_{13} & b_{31}b_{14} \\ b_{41}b_{12} & b_{41}b_{13} & b_{41}b_{14} \end{bmatrix}$$

Equating above two equations we get

$$b_{21}b_{12} = 9, b_{21}b_{13} = 12, b_{21}b_{14} = 16, b_{31}b_{12} = 10, b_{41}b_{12} = 13$$

If

$$b_{21} = 1, \text{then } b_{12} = 9, b_{13} = 12, b_{14} = 16,$$

$$b_{31} = \frac{10}{9} = 3, b_{41} = \frac{13}{9} = 9$$

$$Therefore, B = \begin{bmatrix} 13 & 9 & 12 & 16 \\ 1 & 6 & 1 & 7 \\ 3 & 15 & 4 & 4 \\ 9 & 11 & 9 & 13 \end{bmatrix}$$

Example:3 (For modulo 26)

Take seed number, $b = 7$ and multiplying factor, $t = 3$. Let B is a 4×4 involutory matrix, i.e.

$$B = \begin{bmatrix} b_{11} & \vdots & b_{12} & b_{13} & b_{14} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ b_{21} & \vdots & b_{22} & b_{23} & b_{24} \\ b_{31} & \vdots & b_{32} & b_{33} & b_{34} \\ b_{41} & \vdots & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

is partitioned to

$$\begin{bmatrix} A_{11} & \vdots & A_{12} \\ \cdots & \vdots & \cdots \\ A_{21} & \vdots & A_{22} \end{bmatrix}$$

$$A = \begin{bmatrix} b & bt & bt^2 \\ bt^3 & bt^4 & bt^5 \\ bt^6 & bt^7 & bt^8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 & 21 & 11 \\ 7 & 21 & 11 \\ 7 & 21 & 11 \end{bmatrix}$$

$$So, A_{22} = A + I = \begin{bmatrix} 8 & 21 & 11 \\ 7 & 22 & 11 \\ 7 & 21 & 12 \end{bmatrix}$$

The eigenvalues of A_{22} are $1, 1, 14$.

Therefore,

$$A_{11} = [b_{11}] = [-14] = [12] = 12. \; and$$

$$A_{21}A_{12} = I - A_{22}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 2 & 3 & 9 \\ 1 & 4 & 9 \\ 1 & 3 & 10 \end{bmatrix} = \begin{bmatrix} 25 & 23 & 17 \\ 25 & 23 & 17 \\ 25 & 23 & 17 \end{bmatrix}$$

Now,

$$A_{21}A_{12} = \begin{bmatrix} b_{21} & 0 & 0 \\ b_{31} & 0 & 0 \\ b_{41} & 0 & 0 \end{bmatrix} \begin{bmatrix} b_{12} & b_{13} & b_{14} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} b_{21}b_{12} & b_{21}b_{13} & b_{21}b_{14} \\ b_{31}b_{12} & b_{31}b_{13} & b_{31}b_{14} \\ b_{41}b_{12} & b_{41}b_{13} & b_{41}b_{14} \end{bmatrix}$$

Equating above two equations, we get

$$b_{21}b_{12} = 25, b_{21}b_{13} = 23, b_{21}b_{14} = 17, b_{31}b_{12} = 25, b_{41}b_{12} = 25$$

If

$$b_{21} = 1, then \; b_{12} = 25, b_{13} = 23, b_{14} = 17$$

$$b_{31} = \frac{25}{25} = 1, b_{41} = 1$$

$$Therefore, B = \begin{bmatrix} 12 & 25 & 23 & 17 \\ 1 & 8 & 21 & 11 \\ 1 & 7 & 22 & 11 \\ 1 & 7 & 21 & 12 \end{bmatrix}$$

Example:4 (For modulo 13)

Take seed number, $b = 4$ and multiplying factor, $t = 7$. Let B is a 4×4 involutory matrix, i.e.

$$B = \left[\begin{array}{c:ccc} b_{11} & b_{12} & b_{13} & b_{14} \\ \hdots & \hdots & \hdots & \hdots \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{array}\right]$$

is partitioned to

$$\left[\begin{array}{c:c} A_{11} & A_{12} \\ \hdots & \hdots \\ A_{21} & A_{22} \end{array}\right]$$

$$A = \begin{bmatrix} b & bt & bt^2 \\ bt^3 & bt^4 & bt^5 \\ bt^6 & bt^7 & bt^8 \end{bmatrix} \bmod 13 = \begin{bmatrix} 4 & 2 & 1 \\ 7 & 10 & 5 \\ 9 & 11 & 12 \end{bmatrix}$$

$$A_{22} = A + I = \begin{bmatrix} 5 & 2 & 1 \\ 7 & 11 & 5 \\ 9 & 11 & 0 \end{bmatrix}$$

The eigenvalues of A_{22} are $1, 1, 1$. Therefore,

$$A_{11} = [b_{11}] = [-1] = [12] = 12$$

and

$$A_{21}A_{12} = I - A_{22}^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 9 & 4 & 2 \\ 1 & 8 & 10 \\ 5 & 9 & 12 \end{bmatrix} = \begin{bmatrix} -8 & -4 & -2 \\ -1 & -7 & -10 \\ -5 & -9 & -11 \end{bmatrix} = \begin{bmatrix} 5 & 9 & 11 \\ 12 & 6 & 3 \\ 8 & 4 & 2 \end{bmatrix}$$

Now,

$$A_{21}A_{12} = \begin{bmatrix} b_{21} & 0 & 0 \\ b_{31} & 0 & 0 \\ b_{41} & 0 & 0 \end{bmatrix} \begin{bmatrix} b_{12} & b_{13} & b_{14} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} b_{21}b_{12} & b_{21}b_{13} & b_{21}b_{14} \\ b_{31}b_{12} & b_{31}b_{13} & b_{31}b_{14} \\ b_{41}b_{12} & b_{41}b_{13} & b_{41}b_{14} \end{bmatrix}$$

Equating above two equations, we get

$$b_{21}b_{12} = 5, b_{21}b_{13} = 9, b_{21}b_{14} = 11, b_{31}b_{12} = 12, b_{41}b_{12} = 8$$

If

$$b_{21} = 1, \text{ then } b_{12} = 5, b_{13} = 9, b_{14} = 11,$$

$$b_{31} = \frac{12}{5} = 5, b_{41} = \frac{8}{5} = 12.$$

$$B = \begin{bmatrix} 12 & 5 & 9 & 11 \\ 1 & 5 & 2 & 1 \\ 5 & 7 & 11 & 5 \\ 12 & 9 & 11 & 0 \end{bmatrix}$$

2.4 Proposed Algorithm for Permutation Matrix Generation

This scheme makes use of random permutations of columns and rows of a matrix to form a different key for each data encryption. Permutation matrix formulation scheme is described as follows:

If a matrix A is involutory, then PAP is also involutory, when P is a permutation matrix.

Proof: $(PAP)^{-1} = P^{-1}A^{-1}P^{-1} = PAP$, since $P^{-1} = P$.

Example:

Let $P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$.

$$PAP = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 10 & 11 & 12 & 6 \\ 1 & 2 & 7 & 10 \\ 4 & 5 & 10 & 11 \\ 12 & 12 & 6 & 4 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 12 & 6 & 10 & 11 \\ 7 & 10 & 1 & 2 \\ 10 & 11 & 4 & 5 \\ 6 & 4 & 12 & 12 \end{bmatrix} = \begin{bmatrix} 10 & 11 & 4 & 5 \\ 6 & 4 & 12 & 12 \\ 12 & 6 & 10 & 11 \\ 7 & 10 & 1 & 2 \end{bmatrix}.$$

If the dimension of matrix is $m \times m$, then $m!$ number of permutation matrix and $m!$ number of involutory matrix will be generated using the same element.

2.5 Image Encryption Using Advanced Hill Cipher Algorithm and its FPGA Implementation

The conventional Hill cipher technique has a limitation to encrypt images if the image consists of large area covered with same color or gray level. To overcome the problems of encrypting the images, a new Hill cipher encryption technique has been proposed which uses an involutory key matrix and this scheme also encrypts the images with homogeneous background. A comparative study of the proposed encryption scheme and the Hill cipher is made. The encrypted images reveal that the proposed technique is seen to be more reliable. The block diagram for encryption and decryption of proposed advanced Hill cipher algorithm is shown in Figure 2.1 and 2.2 respectively.

2.5.1 Proposed Advanced Hill Cipher Algorithm

Encryption Algorithm

1. An involutory key matrix of dimensions $k \times k$ is first constructed (involutory key matrix generation method already presented in Section 2.3).

2. Then generate a permutation key matrix of order $k \times k$ (permutation key matrix generation method already presented in Section 2.4).

3. The original image is converted into gray image.

4. Find gray image resolution and then divide into number of blocks of size $k \times k$ each (if necessary, provide padding).

5. The j^{th} pixels of each block are brought together to form a temporary block.

    - Hill cipher technique is applied onto the temporary block.

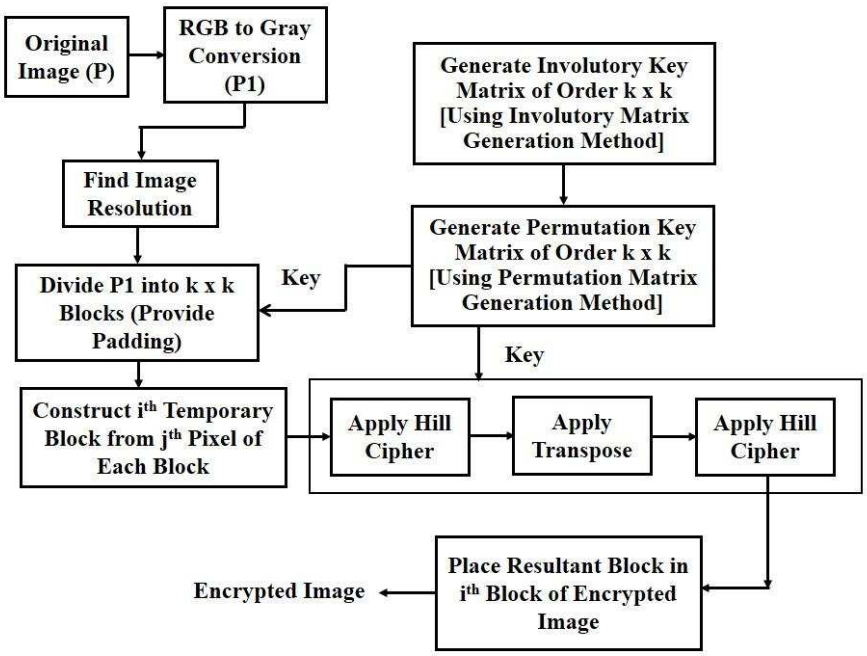


Figure 2.1: Block diagram for encryption of proposed advanced Hill cipher algorithm.

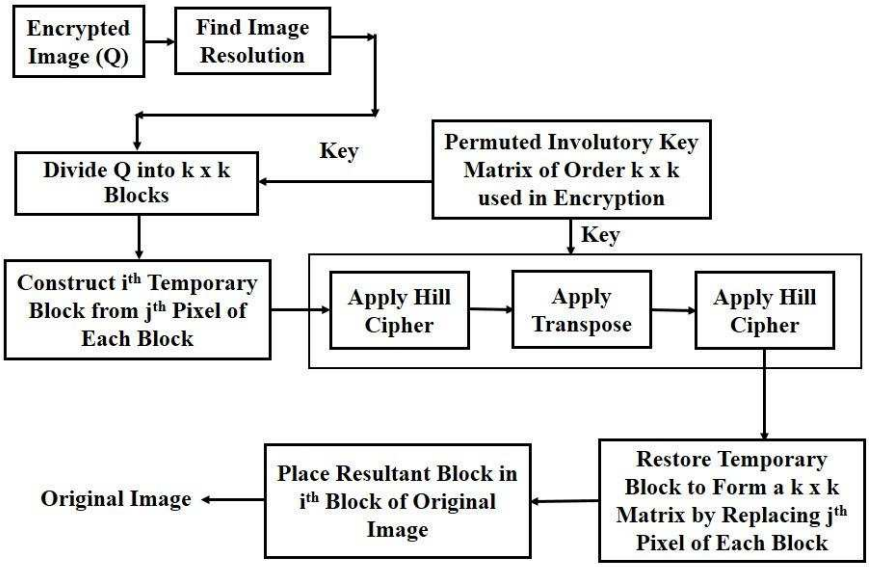


Figure 2.2: Block diagram for decryption of proposed advanced Hill cipher algorithm.

- The resultant matrix is transposed and Hill cipher is again applied to this matrix.

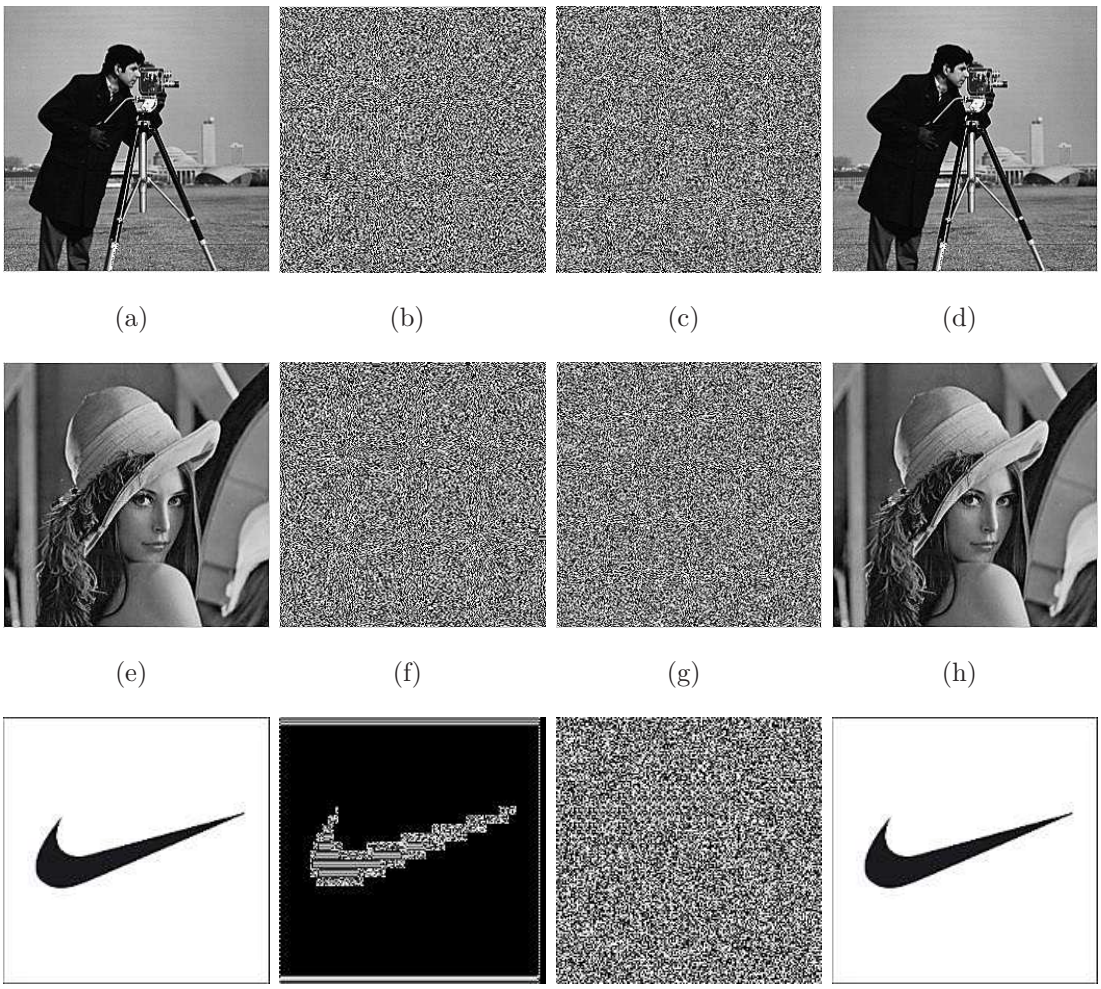
6. The final matrix obtained is placed in the i^{th} block of the encrypted image.
7. The steps 5 to 6 are repeated by incrementing the value of i till the whole image is encrypted.
8. Finally encrypted image is obtained.

Decryption Algorithm

1. Same permuted involutory key matrix of order $k \times k$ is used as in encryption.
2. Find image resolution and then the encrypted image is divided into number of blocks of size $k \times k$ each.
3. The j^{th} pixels of each block are brought together to form a temporary block.
   - Once again Hill cipher technique is applied onto the temporary block.
   - The resultant matrix is transposed and Hill cipher technique is again applied to the resultant matrix to form a temporary block.
4. Temporary block is restored to form $k \times k$ blocks by replacing j^{th} pixel in each block.
5. Then the final block obtained is placed in the i^{th} block of the decrypted image.
6. The steps 3 to 5 are repeated by incrementing the value of i till the whole image is decrypted.
7. Restore the decrypted image.

2.5.2 Simulation Results and Discussion

Different images are encrypted and decrypted using original Hill cipher and proposed advanced Hill cipher algorithm and the results are shown in Figure 2.3. It is clearly noticeable from the Figure 2.3(j), that original Hill cipher cannot encrypt the images properly if the image consists of large area covered with same colour or gray level. But the proposed algorithm works for any images with different gray scale. In Figure 2.3(c, g, k), it is found that proposed advanced Hill cipher algorithm can able to encrypt the images properly as compared to original Hill cipher algorithm.



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Figure 2.3: (a, e, i) Original 'Cameraman', 'Lena' and 'Nike' images , (b, f, j) Encrypted images using original Hill cipher algorithm, (c, g, k) Encrypted images using proposed advanced Hill cipher algorithm, and (d, h, l) Decrypted images using proposed advanced Hill cipher algorithm

2.5.3 Security Analysis

Security is the main thrust of the encryption techniques. Some security analysis has been performed on the proposed encryption technique which includes key space, statistical (histogram, scattered diagram, correlation coefficient) analysis, differential analysis and entropy measure. The security analyses for the proposed technique are discussed as follows.

Key Space Analysis

Key space size indicates the total number of different keys that can be associated with the encryption framework. For a secure encryption framework, the key space should be large enough to make brute-force attacks infeasible. From the cryptographic point of view, the size of the key space should not be smaller than 2^{100} to provide a high level of security [95]. The proposed advanced Hill cipher algorithm is more secure to brute force attacks as compared to original Hill cipher algorithm. A brute-force attack requires $2^{7+8(n/2)^2}$ number of key generations; where n is the order of key matrix. Advanced Hill cipher is a fast encryption technique which can provide satisfactory results against the original Hill cipher technique. The proposed scheme is resistant against known plaintext attack.

Statistical Analysis

In order to resist the statistical attacks, the encrypted images should possess certain random properties.

Histogram of Encrypted Image

In order to appear random, the histograms of the encrypted images should be uniformly distributed in all gray levels. Figure 2.4, 2.5, and 2.6 show the histograms of original, encrypted, and decrypted images using proposed advanced Hill cipher technique. Comparison of the gray histogram has been performed for the image before and after encryption to analyze the statistical performance. Figure 2.4(a), 2.5(a), and 2.6(a) shows the gray histograms of the original images and Figure 2.4(b), 2.5(b), and 2.6(b) shows the gray histograms of the encrypted images. From the two figures, it is clear that the original pixel gray values are concentrated on some value, but the pixel gray values after the encryption are scattered in the entire pixel value space, namely, two images have lower similarity. Clearly, it is difficult to use the statistical performance of the pixel gray value to recover the original image. Thereby, the proposed advanced Hill cipher algorithm has strong ability of resisting statistical attack. From the histograms of Figure 2.4(c), 2.5(c), and 2.6(c) it shows that there is no loss of data during decryption in the proposed advanced Hill cipher algorithm. So the proposed method is applicable to protect both conventional and biometric images during communication and transmission. Figure 2.7 (a, c, e) shows the scattered diagram between original and encrypted images using advanced Hill cipher method.

It finds that, the points are not in a line, it spreads throughout the surface. That means weaker correlation occurs between original and encrypted images. Figure 2.7 (b, d, f) shows the scattered diagram between original and decrypted images using advanced Hill cipher method. It finds that, all the points are along a line. That means stronger correlation occurs between original and decrypted images.

Correlation of Adjacent Pixels

The proposed advanced Hill cipher image encryption system should be resistant to statistical attacks. Correlation coefficients of pixels in the encrypted image should be as low as possible [96, 97]. Horizontal, vertical, and diagonal correlation coefficients (r_{xy}) of two adjacent pixels can be calculated using the following equations:

$$r_{xy} = \frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.9}$$

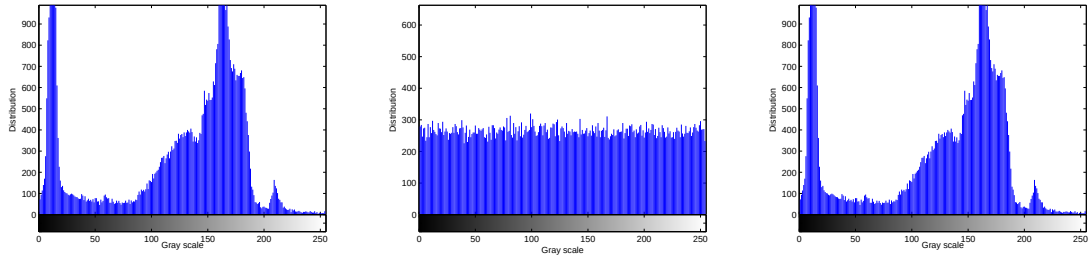
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2 \tag{2.10}$$

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{2.11}$$

where x and y are gray-scale values of two adjacent pixels in the image and E denotes the expectation operator shown in

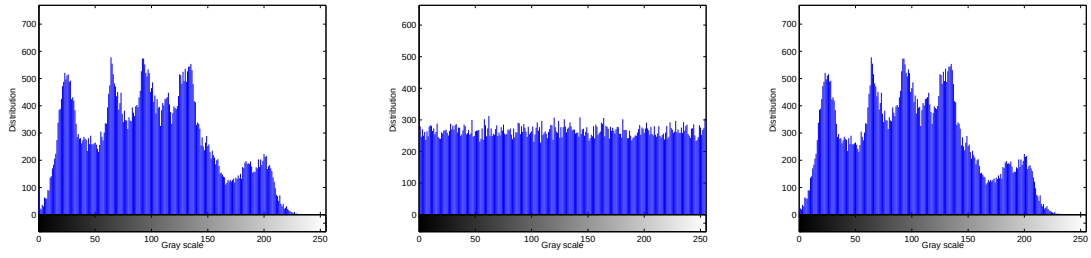
$$E(z) = \frac{1}{N}\sum_{i=1}^{N} z_i \tag{2.12}$$

About a thousand pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels are randomly selected from the encrypted image, and the correlation coefficients are calculated, respectively [98]. The results are shown in Table 2.1. From Table 2.1 it is concluded that the correlation coefficient of original images is almost close to 1 and the correlation coefficient of encrypted images using proposed advanced Hill cipher method is close to 0 in all the three directions that means no similarity occurs between original images and encrypted images whereas the correlation coefficient of encrypted image using Hill cipher method for 'Nike' image is not close to 0 that means close to 1, which shows that some similarity occurs between original image and encrypted image but for 'Cameraman' and 'Lena' encrypted images its close to 0 that means no similarity occurs between original and encrypted image. It is clearly noticeable form the result of Table 2.1 is that original Hill cipher fails to encrypt the images properly if the image consists of large area covered with same color or gray level. But



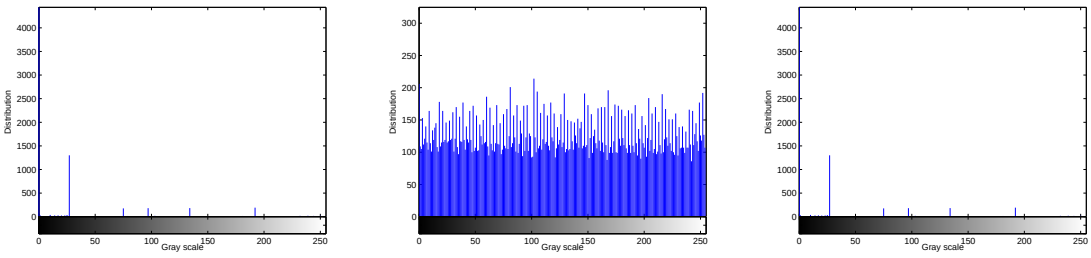
(a) (b) (c)

Figure 2.4: Histograms of *'Cameraman'* image: (a) Histogram of original image, (b) Histogram of corresponding encrypted image, (c) Histogram of corresponding decrypted image by using proposed advanced Hill cipher algorithm



(a) (b) (c)

Figure 2.5: Histograms of *'Lena'* image: (a) Histogram of original image, (b) Histogram of corresponding encrypted image, (c) Histogram of corresponding decrypted image by using proposed advanced Hill cipher algorithm



(a) (b) (c)

Figure 2.6: Histograms of *'Nike'* image: (a) Histogram of original image, (b) Histogram of corresponding encrypted image, (c) Histogram of corresponding decrypted image by using proposed advanced Hill cipher algorithm

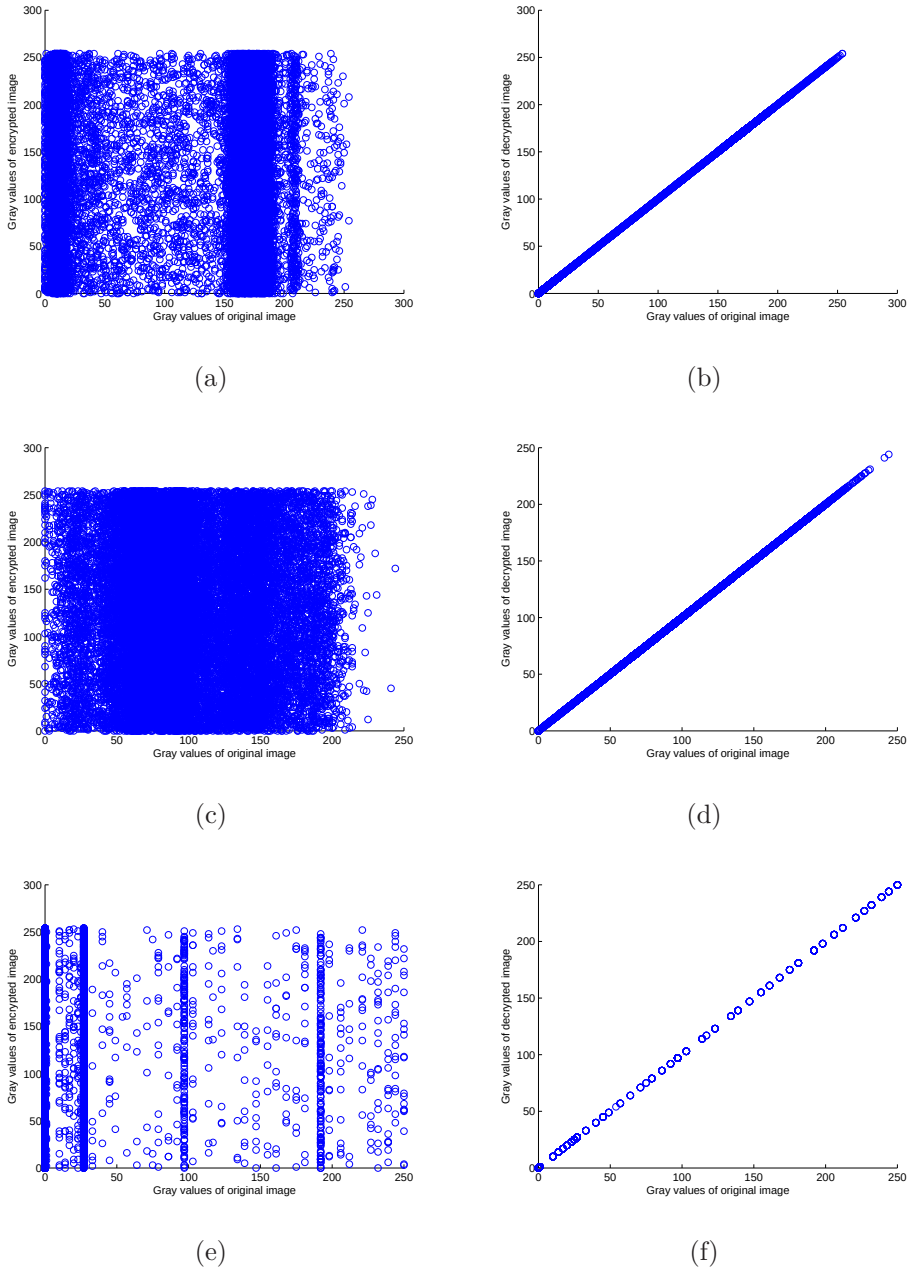
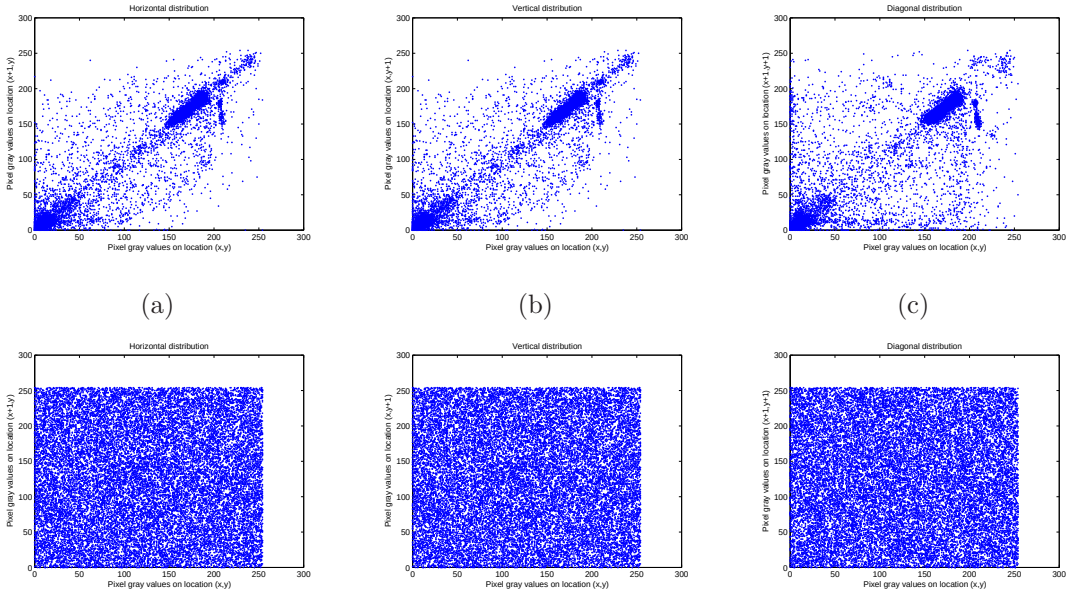


Figure 2.7: (a, c, e) Scattered diagram between original and encrypted images of 'Cameraman', 'Lena', and 'Nike' respectively using advanced Hill cipher method, (b, d, f) Scattered diagram between original and decrypted images of 'Cameraman', 'Lena', and 'Nike' respectively using advanced Hill cipher method

the proposed advanced Hill cipher algorithm works for any images with same color or gray level. Finally from the tabulated data, it is concluded that adjacent pixels of original image have very strong linear correlation, while the correlation between adjacent pixels of encrypted image using proposed advanced Hill cipher method is

very small. It has damaged the linear correlation of original image. Therefore the proposed encrypted algorithm can effectively resist pixel correlation statistical attack. Figure 2.8, 2.9, and 2.10 shows the correlation distribution of two adjacent pixels for 'Cameraman', 'Lena', and 'Nike' images respectively. From the contrast diagrams it is observed that the correlation between pixels of original image is much larger than the correlation between pixels of encryption image. That means, the adjacent pixels of original image have very strong linear correlation, while the correlation between adjacent pixels of encrypted image is very small. It has damaged the linear correlation of original image. Therefore the propose encrypted algorithm can effectively resist pixel correlation statistical attack.



(a) (b) (c)

(d) (e) (f)

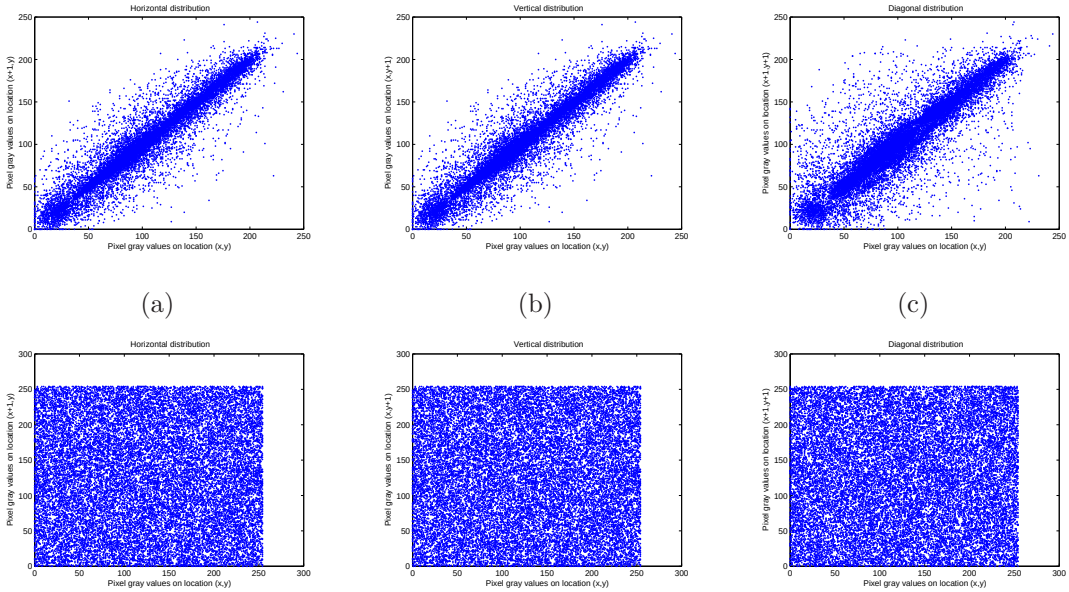
Figure 2.8: Correlation distribution of two adjacent pixels for 'Cameraman' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image by using proposed advanced Hill cipher algorithm

Differential Analysis

The major requirement of all the encryption techniques is the encrypted image should be significantly different to the original one. To quantify the difference between encrypted image and corresponding original image, three measures were used: Mean

Table 2.1: Comparison of correlation coefficients between original Hill cipher algorithm and proposed advanced Hill cipher algorithm.

Correlation coefficient	Original images			Encrypted images using original Hill cipher			Encrypted images using advanced Hill cipher		
	Cameraman	Lena	Nike	Camera man	Lena	Nike	Camera man	Lena	Nike
Horizontal (H)	0.9168	0.9384	0.9466	0.1209	0.0328	0.7973	-0.0027	0.0007	0.0074
Vertical (V)	0.9490	0.9698	0.9111	0.1129	0.1115	0.7033	-0.0049	0.0008	-0.0043
Diagonal (D)	0.8835	0.9164	0.8421	0.0034	-0.0117	0.6679	-0.0039	0.0069	0.0031
$(H^2 + V^2 + D^2)^{0.5}$	1.5880	1.6313	1.5606	0.1654	0.1168	1.2555	0.0068	0.0069	0.0091
Average (H, V, D)	0.9165	0.9415	0.9000	0.0791	0.0442	0.7228	-0.0038	0.0028	0.0021



(a) (b) (c)

(d) (e) (f)

Figure 2.9: Correlation distribution of two adjacent pixels for 'Lena' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image by using advanced Hill cipher algorithm

Absolute Error (MAE), the Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI).

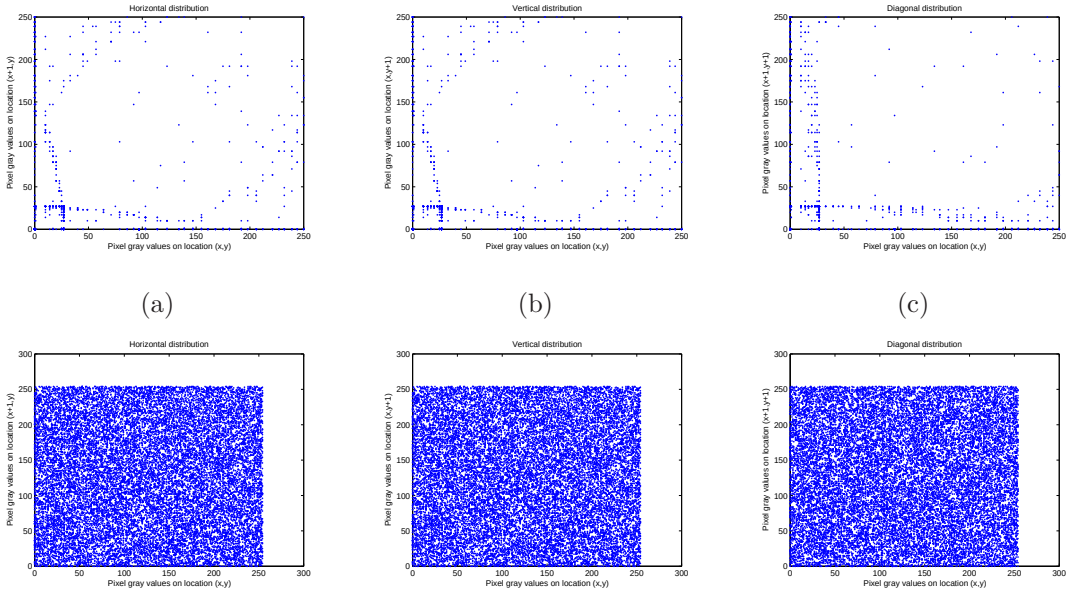
The MAE between original image and encrypted image is defined as

$$MAE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} |a_{ij} - b_{ij}| \tag{2.13}$$

where $M \times N$, size of the original and encrypted images. The parameters a_{ij} and b_{ij} are gray scale values of pixels in original and encrypted images, respectively. The larger the MAE value, the better the encryption security.

The $NPCR$ is used to measure the number of pixels in difference of gray level in two images. Let $C_1(i,j)$ and $C_2(i,j)$ be the gray level of the pixels at the i^{th} row and j^{th} column of two images C_1 and C_2, respectively. The $NPCR$ of these two images is defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100 \tag{2.14}$$



(a) (b) (c)

(d) (e) (f)

Figure 2.10: Correlation distribution of two adjacent pixels for 'Nike' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image by using advanced Hill cipher algorithm

where N is the total number of pixels in the image and $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases}$$

The expected that means the ideal value of $NPCR$ is found to be 99.61%.

Another measure, UACI, is defined as the average intensity of difference in a gray level of corresponding pixels between the two images C_1 and C_2. The UACI of these two images is defined as

$$UACI = \frac{1}{N}\left[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{2^L - 1}\right] \times 100 \tag{2.15}$$

In the proposed method, $L = 8$ bits, so $2^L - 1 = 255$. The expected that means the ideal value of UACI is found to be 33.46%. Apart from this PSNR measure is also used to show the efficacy of the proposed method.

The comparison of NPCR, UACI, MAE, and PSNR criteria of different images using the proposed advanced Hill cipher method and the original Hill cipher algorithm is tabulated in Table 2.2.

Table 2.2: Comparison of NPCR, UACI, MAE, and PSNR criteria of proposed advanced Hill cipher algorithm and the original Hill cipher algorithm

Criteria (expected value)		Original Image Vs. Encrypted Image	
		Original Hill cipher	Advanced Hill cipher
NPCR (99.61%)	Cameraman	99.5789	99.5941
	Lena	99.5560	99.6323
	Nike	14.2239	99.3834
UACI (33.46%)	Cameraman	29.2526	31.3096
	Lena	29.1170	30.3733
	Nike	6.5422	48.4655
MAE (Larger Value)	Cameraman	74.5941	79.8394
	Lena	74.2484	77.4518
	Nike	16.6825	123.5869
PSNR (Smaller Value)	Cameraman	8.8764	8.3890
	Lena	8.9577	8.6414
	Nike	15.0897	4.9776

The NPCR, UACI, and MAE value of proposed advanced Hill cipher is greatly improved as compared to original Hill cipher. In the proposed advanced Hill cipher algorithm, the NPCR value of 'cameraman', and 'Nike' images is nearer equal to the expected NPCR value whereas the NPCR value of 'Lena' image is 0.022% higher than the expected value. Similarly, the UACI value of 'cameraman' and 'lena' is nearer equal to the expected UACI value whereas the UACI value of 'nike' image is around 15% higher than the expected value. The MAE values are larger of all the images. As a result, the proposed advanced Hill cipher algorithm has a good ability to encrypt an image against any attack. PSNR (Peak Signal-to-Noise Ratio) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although

a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better.

But in the proposed algorithm, the PSNR is calculated between original image and encrypted image, as well as original and decrypted image. In encrypted images, the total pixels are disturbed. Therefore, the MSE between original image and encrypted image is very high. Hence the PSNR will be lower. But when we consider PSNR between original and decrypted images, it is found to be very high because the two images are same, and hence MSE is approximately zero. High value MSE and low value PSNR indicates that two images are completely different. On the other hand, high value of PSNR indicates the high quality of image.

When we calculate the MAE between original image and encrypted image, the value of MAE should be larger for better encryption security. Table 2.2 shows that PSNR value is less in advanced Hill cipher algorithm compared to original Hill cipher algorithm.

Measure of Entropy

Entropy is a statistical measure of randomness that can be used to characterize the texture of an image. The entropy of an image A is defined as:

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \tag{2.16}$$

Where H_e is the entropy, G is gray value of input image, $P(k)$ is probability of occurrence of symbol k. Higher value of entropy of encrypted image, better the security. Table 2.3, presents the comparison of entropy between original images and encrypted images using the original Hill cipher algorithm and the proposed advanced Hill cipher algorithm. A higher value of the entropy obtained in case of proposed algorithm as compared to that obtained in the original Hill cipher algorithm indicates that the proposed algorithm introduces more randomness in the encrypted image resulting in better encryption.

Table 2.3: Entropy of original images and encrypted images by using original Hill cipher algorithm, and the proposed advanced Hill cipher algorithm

Images	Entropy		
	Original Image	Encrypted Image	
		Original Hill cipher algorithm	Proposed advanced Hill cipher algorithm
Cameraman	7.1684	7.9569	7.9916
Lena	7.5977	7.9735	7.9915
Nike	0.6896	1.6415	7.9609

2.5.4 FPGA Implementation of Advanced Hill Cipher for Image Encryption

Systolic Architecture Implementation

Systolic architecture [29] is a methodology for mapping high-level computations into hardware structures. In a systolic system, data flows from the computer memory in a recurring way, passing through many processing elements before it returns to memory, much similar to the manner in which blood circulates to and from the heart. The system works like an automobile assemblage line where different people work on the same car at different times and many cars are assembled simultaneously. An assemblage line is always linear; however, systolic systems are sometimes two-dimensional. They can be rectangular, triangular, or hexagonal to make use of higher degrees of parallelism. Moreover, to implement a diversity of computations, data flow in a systolic system may be at different speeds in multiple directions-both inputs and (partial) results flow, whereas only results flow in classical pipelined systems. Generally, a systolic system is easy to implement because of its regularity and easy to reconfigure because of its modularity.

So, in VLSI signal processing, systolic architecture is a proven technique to implement recursive matrix multiplication. The process of matrix multiplication in encryption and decryption is called as recursive matrix multiplication. A systolic array is composed of matrix-like rows of data processing units called cells. Each cell shares the information with its neighbours immediately after processing. The systolic array is often rectangular where data flows across the array between neighbour processing units, often with different data flowing in different directions.

One input matrix is fed in a row at a time from the top of the array and is passed down the array; the other matrix is fed in a column at a time from the left hand side of the array and passes from left to right. The result of the multiplication is stored in the array and can now output a row or a column at a time, flowing down or across the array.

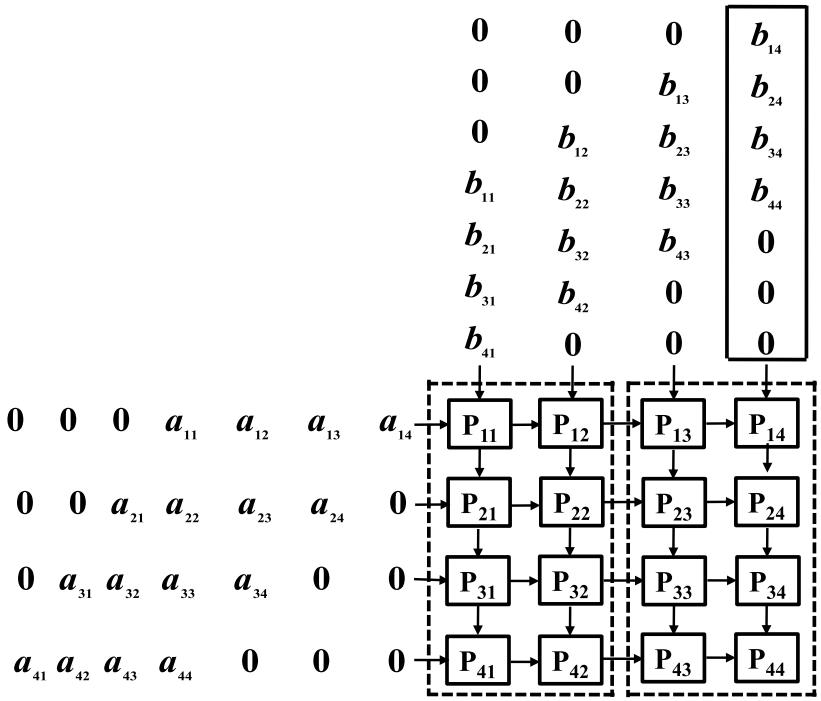


Figure 2.11: Multiplication using systolic architecture

Matrix multiplication using systolic array is depicted in Figure 2.11 P_{11} to P_{44} are processing elements, in which digital multipliers are placed.

Vedic Multiplier Implementation

Multipliers are extensively used in FIR filters, Microprocessors, DSP and communication applications. For higher order multiplications, a huge number of adders or compressors are used to perform the partial product addition. The need of low power and high speed multiplier is increasing as the need of high speed processors are increasing. The Vedic multiplication technique is based on 16 Vedic sutras or aphorisms, which are actually word formulae describing natural ways of solving a whole range of mathematical problems. The mathematical operations using Vedic method are very fast and requires less hardware, which has ability to improve the computational speed of processors.

The ancient Vedic multiplication techniques are equally applicable for binary numbers also. The Vedic mathematics reduces the cumbersome-looking calculations in conventional mathematics to a very simple one. This is so because the Vedic formulae are claimed to be based on the natural principles on which the human mind works. The implemented multiplier is based on Urdhvatiryakbhyam (vertically and crosswise) sutra [40].

Vedic Multiplier for 2×2 Bit Module

The method of multiplication for two, 2-bit numbers A and B where $A = a1a0$ and $B = b1b0$ using Vedic multiplier is shown in Figure 2.12. Firstly, the least significant bits are multiplied which gives the least significant bit of the final product (vertical). Then, the LSB of the multiplicand is multiplied with the next higher bit of the multiplier and added with, the product of LSB of multiplier and next higher bit of the multiplicand (crosswise). The sum gives second bit of the final product and the carry is added with the partial product obtained by multiplying the most significant bits to give the sum and carry. The sum is the third corresponding bit and carry becomes the fourth bit of the final product.
First $s0 = a0b0$
Second with carry $c1s1 = a1b0 + a0b1$
Final with carry $c2s2 = c1 + a1b1$
The final result will be $c2\ s2\ s1\ s0$. This multiplication method is applicable for all the cases.

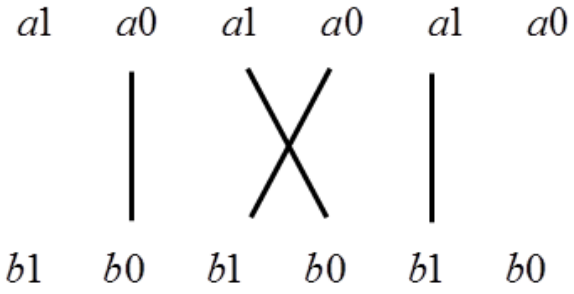


Figure 2.12: The Vedic multiplication method for 2-bit binary numbers

The 2×2 Vedic multiplier module is implemented using four input AND gates and two Half-adders which is as shown in Figure 2.13. It is found that the hardware architecture of 2×2 bit Vedic multiplier is same as the hardware architecture of 2×2 bit conventional array multiplier. Hence it is observed that multiplication of 2 bit

binary numbers by Vedic method does not make significant effect in improvement of the multiplier's efficiency. Very precisely it can be stated that the total delay is only 2-half-adders delay, after final bit products are generated, which is very similar to array multiplier. So switch over to the implementation of 4×4 bit Vedic multiplier which uses the 2×2 bit multiplier as a basic building block. The same method can be extended for input bits 4 and 8. But computation with higher number of bits require slight modification.

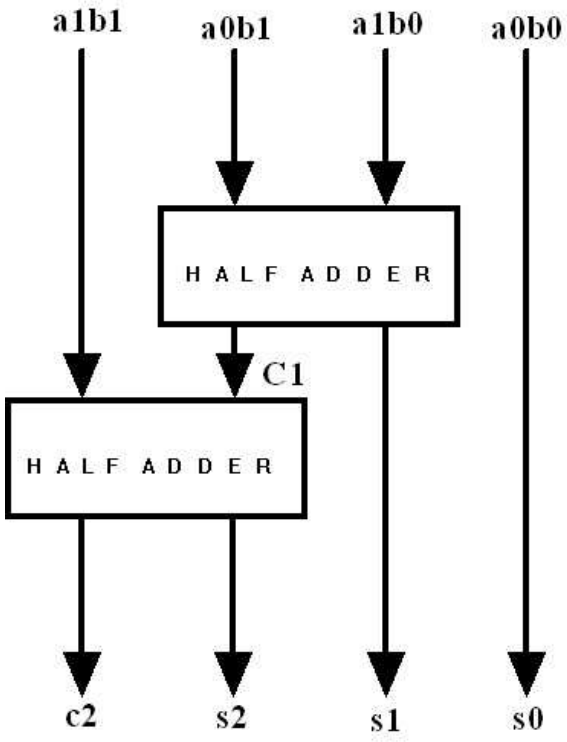


Figure 2.13: Block diagram for 2×2 bit Vedic multiplier

Vedic Multiplier for 4×4 Bit Module

A 4×4 bit Vedic multiplier module was implemented using four 2×2 bit Vedic multiplier modules as discussed in Figure 2.12. Let's analyze 4×4 multiplications, say $A = a3\ a2\ a1\ a0$ and $B = b3\ b2\ b1\ b0$. The output line for the multiplication result is $s7\ s6\ s5\ s4\ s3\ s2\ s1\ s0$. The A and B are divided into two parts, say $a3$ $a2$ and $a1$ $a0$ for A and $b3$ $b2$ and $b1$ $b0$ for B. Using the fundamental of Vedic multiplication, taking two bit at a time and using 2-bit multiplier block, we have the following structure for multiplication, which is presented in Figure 2.14.

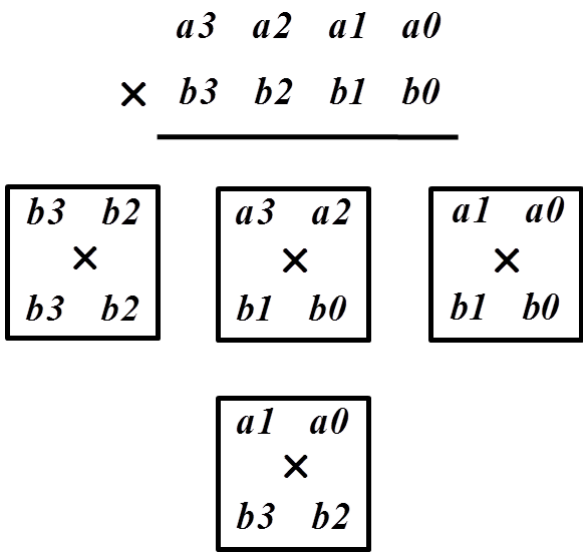


Figure 2.14: Block diagram for 4×4 bit Vedic multiplication

In this figure each block is a 2×2 bit Vedic multiplier. First 2×2 bit multiplier inputs are $a1$ $a0$ and $b1$ $b0$. The last block is 2×2 bit multiplier with inputs $a3$ $a2$ and $b3$ $b2$. The middle one shows two 2×2 bit multiplier with inputs $a3$ $a2$, $b1$ $b0$ and $a1$ $a0$, $b3$ $b2$. So the final result of multiplication, which is of 8 bits, $s7$ $s6$ $s5$ $s4$ $s3$ $s2$ $s1$ $s0$. To get final product ($s7$ $s6$ $s5$ $s4$ $s3$ $s2$ $s1$ $s0$), four 2×2 bit Vedic multiplier (Figure 2.13) and three 4-bit Ripple-Carry (RC) adders are required. The arrangements of RC adders is presented in Figure 2.15, helps us to reduce delay. Similarly, 8×8 Vedic multiplier modules are implemented by using four 4×4 multiplier modules.

Vedic Multiplier for 8×8 Bit Module

The 8×8 bit Vedic multiplier module which is as shown in Figure 2.16 can be easily implemented by using four 4×4 bit Vedic multiplier modules as discussed. Let's analyze 8×8 multiplications, say $A = a7$ $a6$ $a5$ $a4$ $a3$ $a2$ $a1$ $a0$ and $B = b7$ $b6$ $b5$ $b4$ $b3$ $b2$ $b1$ $b0$. The output line for the multiplication result will be of 16 bits as - $s15$ $s14$ $s13$ $s12$ $s11$ $s10$ $s9$ $s8$ $s7$ $s6$ $s5$ $s4$ $s3$ $s2$ $s1$ $s0$. Let's divide A and B into two parts, say the 8 bit multiplicand A can be decomposed into pair of 4 bits AH-AL. Similarly multiplicand B can be decomposed into BH-BL. The 16 bit product can be written as:
$P = A \times B = (AH - AL) \times (BH - BL) = AH \times BH + (AH \times BL + AL \times BH) + AL \times BL$
Using the fundamental of Vedic multiplication, taking four bits at a time and using 4 bit multiplier block as discussed we can perform the multiplication. The outputs

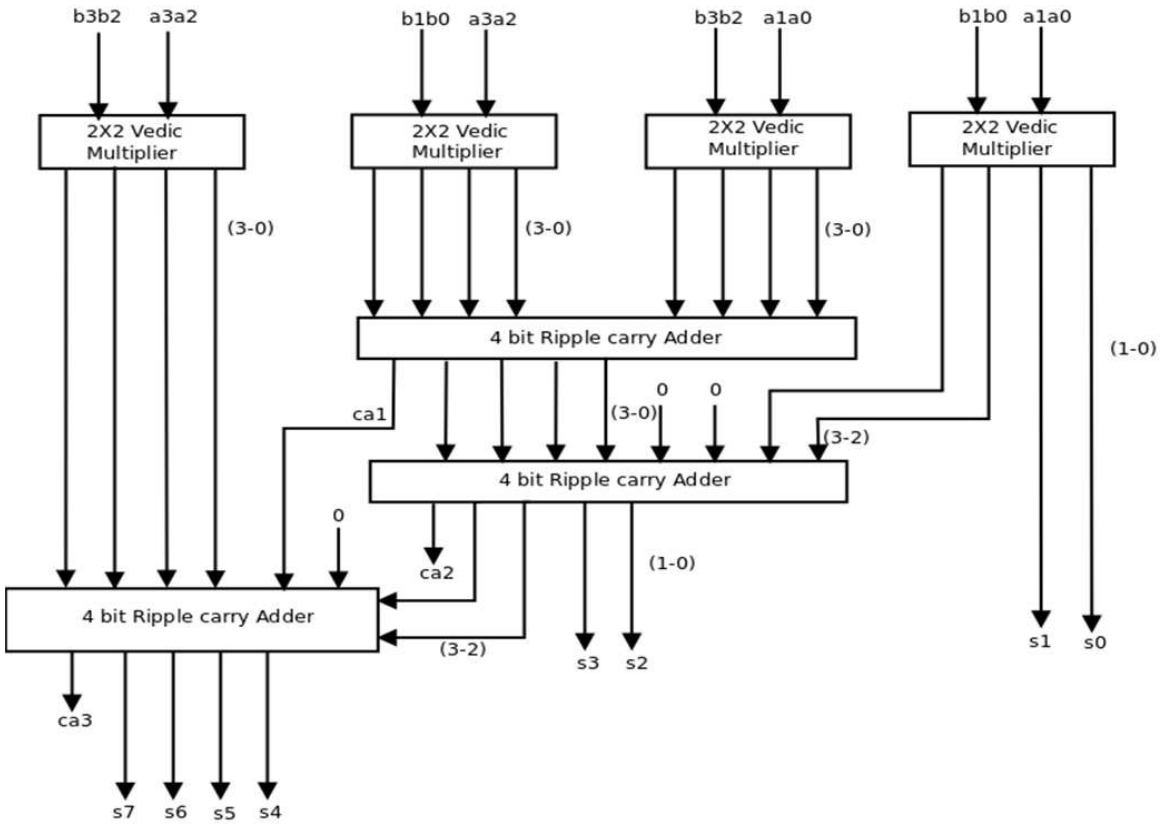


Figure 2.15: Block diagram for 4×4 bit Vedic multiplier

of 4×4 bit multipliers are added accordingly to obtain the final product. Here total three 8-bit ripple-carry adders are required as shown in Figure 2.16.

In this work, Hill cipher algorithm is used, then proposed advanced Hill cipher algorithm for image encryption is employed. The VLSI architecture for Hill cipher and advanced Hill cipher based image encryption is designed, implemented and results are presented.

2.5.5 Results and Discussion

In this work, 256×256 pixel image is used for encryption. Each pixel is represented as 8-bit binary value. Adders and multipliers required to perform matrix multiplication are designed for 8-bit. Image encryption using Hill cipher algorithm is implemented using systolic arrays on FPGA. Systolic arrays contain multipliers. We have used conventional multiplier, Booth Wallace multiplier and Vedic multiplier in processing element of systolic array separately to verify the performance of the Hill cipher implementation. Results are compared with respect to FPGA utilization, power and

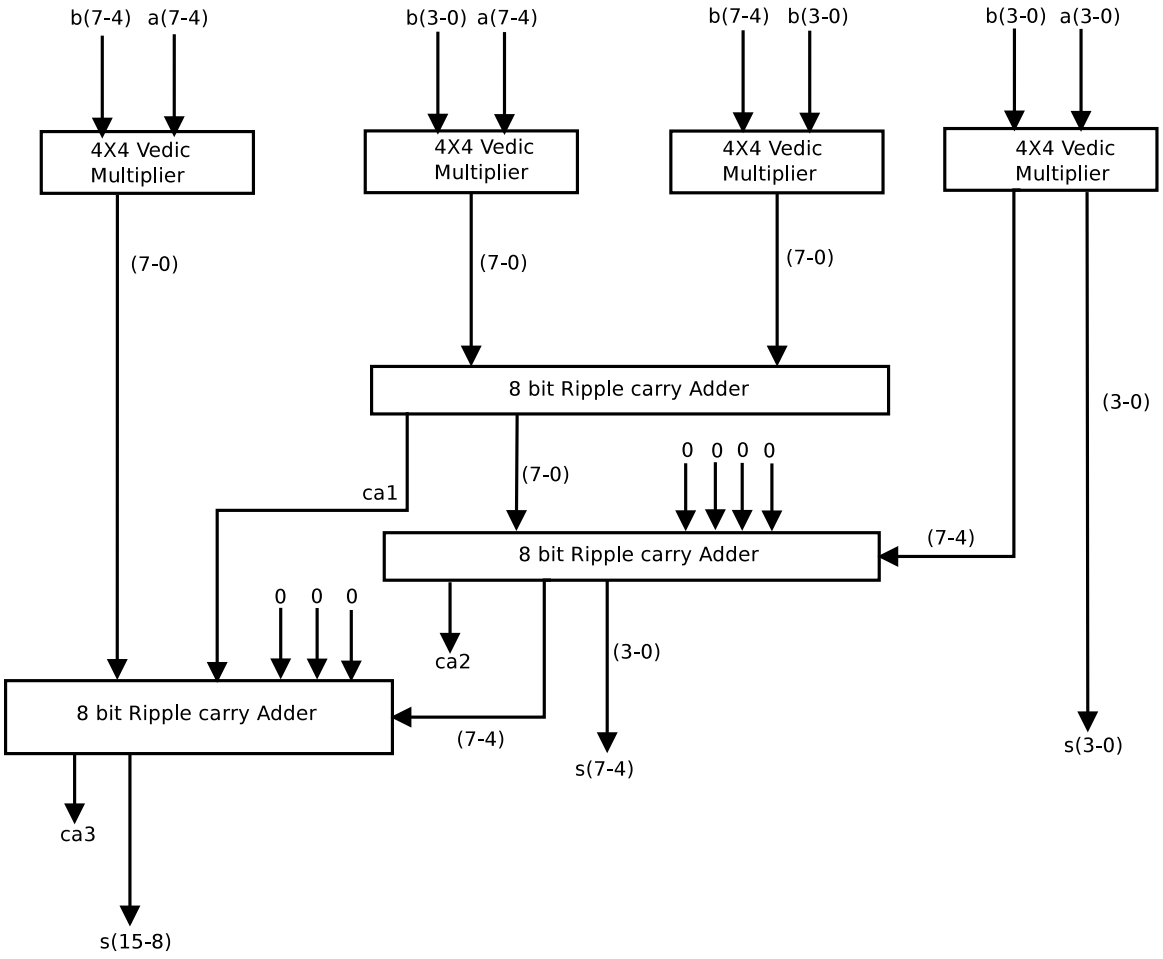


Figure 2.16: Block diagram for 8×8 bit Vedic multiplier

speed of operation. Table 2.4 presents number of multipliers and adders required for implementing Hill cipher for 8-bit multiplication. Table 2.5 and Table 2.6 shows the comparison of conventional array multiplier, Booth Wallace multiplier and Vedic multiplier with respect to number of slices used, maximum combinational path delay and power consumption using Hill cipher algorithm and proposed advanced Hill cipher algorithm respectively.

Booth Wallace results are not included, because it needs Booth encoding process and comparison is not logical.

It is evident from Table 2.4 that, Vedic multiplier uses less number of adders in implementation of Hill cipher.

Vedic multipliers are faster and consume more power than Booth Wallace multiplier in Hill cipher implementation. The FPGA results for proposed advanced Hill cipher are as presented in Table 2.6 in comparison of conventional array multiplier,

Table 2.4: Comparison between conventional array multiplier and Vedic multiplier with respect to number of multipliers and adders used

Input bit Length	Number of Calculations			
8	Conventional Array Multiplier		Vedic Multiplier	
	Multipliers	Adders	Multipliers	Adders
	64	77	64	53

Booth Wallace multiplier and Vedic multiplier with respect to number of slices used, maximum combinational path delay and power consumption.

From the results shown in Table 2.6, it is evident that, Vedic multiplier is a high performance architecture. There is always trade-off between area, power and timing in hardware implementations.

2.6 Image Encryption by H-S-X Cryptosystem and Its FPGA Implementation

Noninvertible key matrix over Z_m is the main disadvantage of Hill cipher, because few of the matrices have inverses over Z_m . This means that the encrypted text can not be decrypted. Moreover, Hill cipher algorithm cannot encrypt images that contain large areas of a single colour. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. To overcome the problems of encrypting the images, a novel H-S-X (Hill-Shift-XOR)cryptosystem has been proposed. The scheme is relatively slow but quite reliable technique where cryptanalysis is quite difficult. It also injects more diffusion and confusion which are the two important attributes of a powerful encryption technique. A comparative study of the proposed encryption scheme and the existing Hill cipher scheme is made. The output encrypted images reveal that the proposed technique is quite reliable and robust.

As we note that Hill cipher can be adopted to encrypt grayscale and colour images, proposed H-S-X cryptosystem can also be used for grayscale and colour images. In this technique, encryption is done in 3 sub-steps. These steps if repeated sufficiently leads to quite a strong encryption at the cost of encryption time. The proposed algorithm is resistant to brute-force attacks, known plaintext attacks as well as chosen plaintext attacks. The block diagram for the proposed H-S-X cryptosystem is shown in Figure

Table 2.5: Comparison of conventional array multiplier, Booth Wallace multiplier and Vedic multiplier method with respect to number of slices used, maximum combinational path delay and power consumption using Hill cipher algorithm (FPGA frequency: 100MHz)

Sl. No.	Method	No. of slices used in Virtex-II Pro FPGA	Maximum combinational path delay	Power calculated using Xpower tool (Xilinx)
1.	Conventional Array Multiplier	268	356ns	240.4mW
2.	Booth Wallace Multiplier	347	220ns	90.29mW
3.	Vedic Multiplier	298	129ns	140.34mW

2.17.

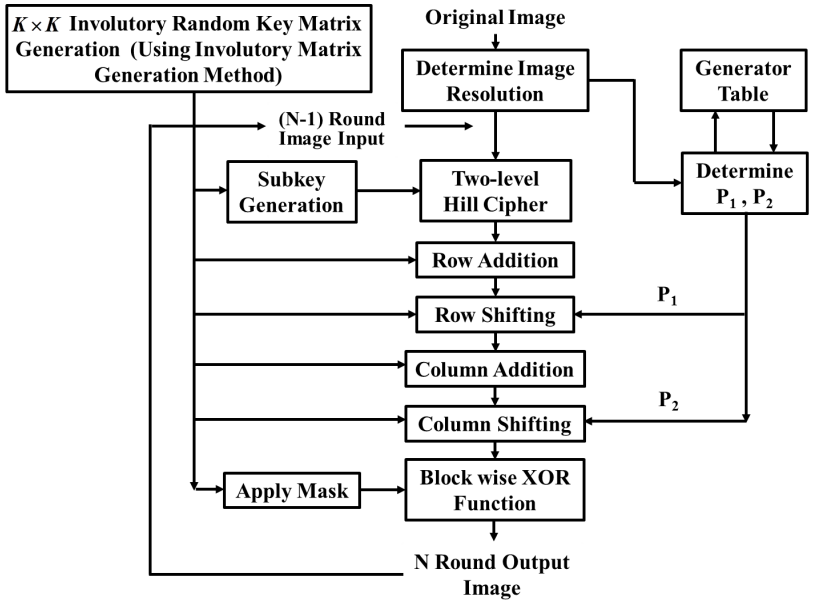


Figure 2.17: Block diagram for proposed H-S-X cryptosystem.

Table 2.6: Comparison of conventional array multiplier, Booth Wallace multiplier and Vedic multiplier method with respect to number of slices used, maximum combinational path delay and power consumption using proposed advanced Hill cipher algorithm(FPGA frequency: 100MHz)

Sl.No.	Method	No. of slices used in Virtex-II Pro FPGA	Maximum combinational path delay	Power calculated using Xpower tool (Xilinx)
1	Conventional Array Multiplier	616	1067ns	660.5mW
2	Booth Wallace Multiplier	774	795ns	519.4mW
3	Vedic Multiplier	676	613ns	590.8mW

2.6.1 Proposed H-S-X Cryptosystem

1. 2-level Hill ciphers is applied to original image using a preferably random matrix (having odd determinant).

2. Key will get added to the first row of matrix generated out of two level Hill cipher. m rows in the key will get added to first row of matrix (output of two level Hill cipher) m times. Each row of intermediate cipher matrix is added with each row of the key matrix.

3. Similar operation is performed for columns as like as step 2.

4. Appropriate P_1 and P_2 values are selected for the row and column shifting function where, P_1 and P_2 are generators for the elements co-prime to congruence modulo n and m respectively. These values can be extracted from a predetermined table for different n values.

   (a) i^{th} row pixel values circularly down shifted according to the formula

$$\left|P_1^{i+1} + ceil\left(i/k\right) * k_{r_{i(\bmod k)}}\right| (\bmod n) \tag{2.17}$$

where,

i - Corresponding row number,

k - Size of key matrix used for shifting,

$k_{r_{i(\bmod k)}}$ - Sum of the values of the i^{th} row of the key matrix,

n - Number of columns in the original image,

P_1 - Generator for co-prime numbers congruence modulo n,

$ceil()$ The ceiling Function.

(b) j^{th} column pixel values circularly right shifted according to the formula

$$\left|P_2^{j+1} + ceil\left(j/k\right) * k_{c_{j(\bmod k)}}\right| (\bmod m) \tag{2.18}$$

where,

j - Corresponding column number,

k - Size of key matrix used for shifting,

$k_{c_{j(\bmod k)}}$ - Sum of the values of the j^{th} column of the key matrix,

m - Number of columns in the original image,

P_2 - Generator for co-prime numbers congruence modulo m,

$ceil()$ - The ceiling Function.

5. Block wise XOR operation is performed onto resultant image using the key matrix or one of its permutations or a masked version of the key. All the above operations are performed modulo 256 and on 8-bit gray (or 24-bit colour) images.

2.6.2 Simulation Results and Discussion

Different images are encrypted and decrypted using original Hill cipher and proposed H-S-X cryptosystem and the results are shown in Figure 2.18 and Figure 2.19. It is clearly noticeable from the Figure 2.18(b, f), that original Hill cipher cannot encrypt the images properly if the image consists of large area covered with same color or gray level. But proposed H-S-X cryptosystem works fine for all types of images including gray scale, color and also binary images. In Figure 2.18(c, g, k),

it is found that proposed H-S-X algorithm can able to encrypt the images properly as compared to original Hill cipher algorithm. Figure 2.19 shows encryption and decryption result of color image by using original Hill cipher algorithm and prposed H-S-X cryptosystem. Prposed H-S-X cryptosystem also can encrypt color images and its results are presented in Figure 2.19(c). The palmprint biometric image is taken from the CASIA (Chinese Academy of Sciences' Institute of Automation) image database [99].

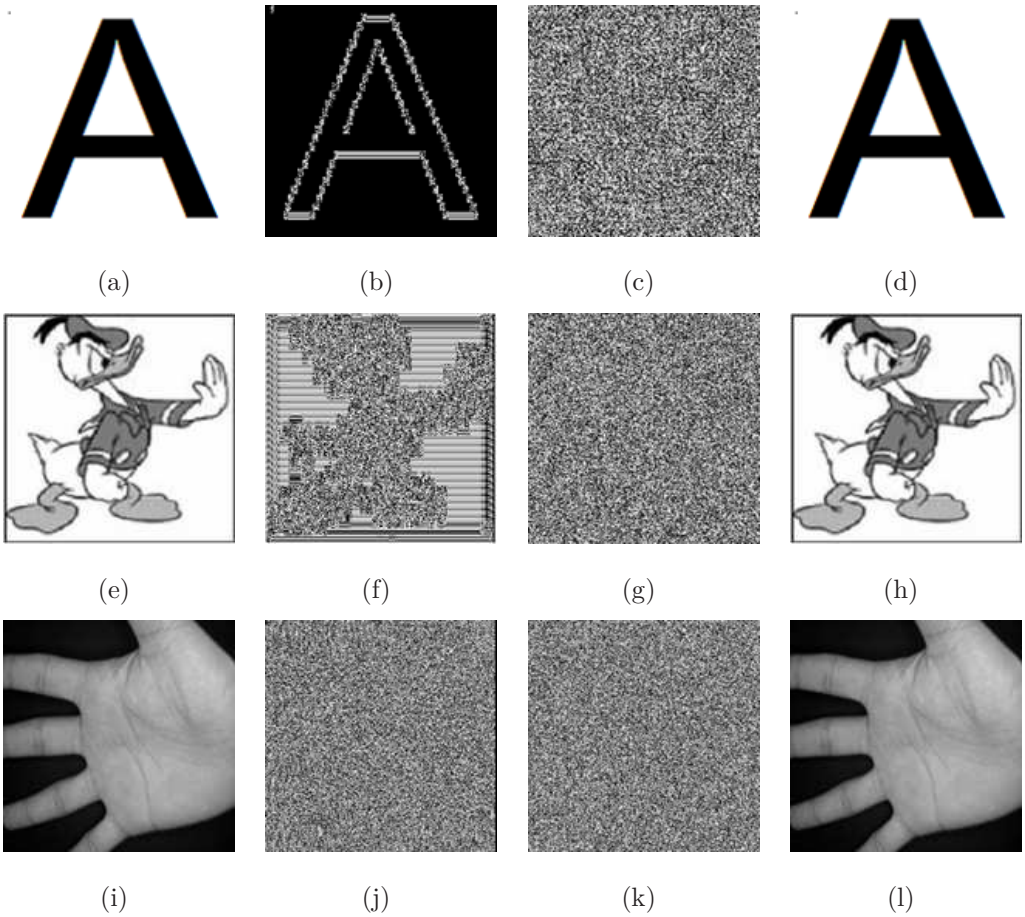
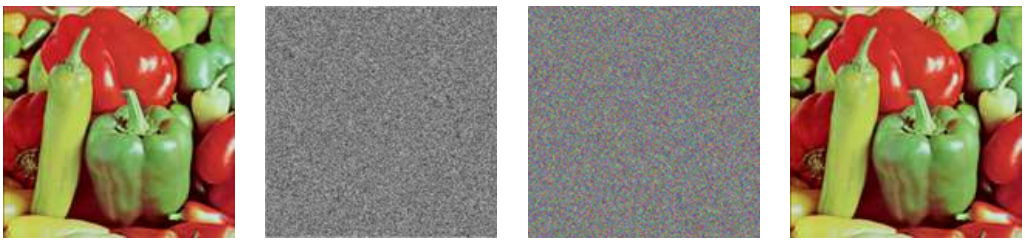


Figure 2.18: (a, e, i) Original images of 'Capital A', 'Duck', and 'Palmprint', (b, f, j) Corresponding encrypted images by original Hill cipher, (c, g, k) Corresponding encrypted images by proposed H-S-X cryptosystem, and (d, h, l) Corresponding decrypted images by proposed H-S-X cryptosystem.

2.6.3 Security Analysis

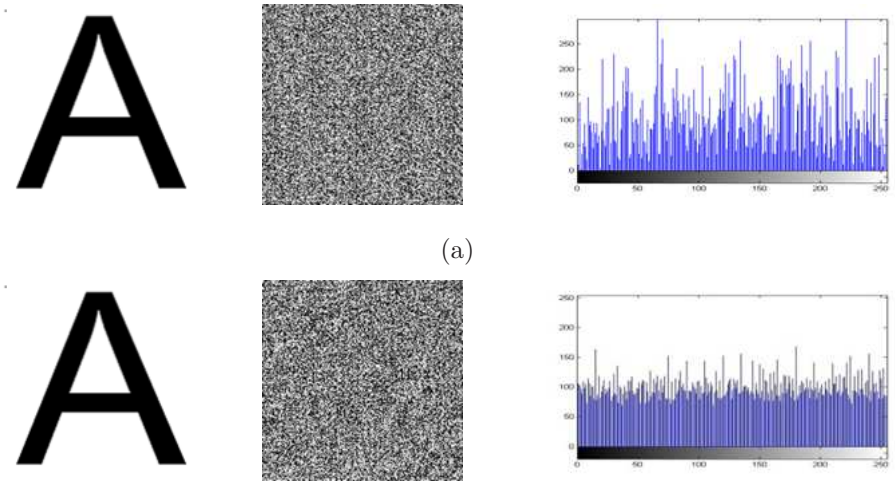
The proposed scheme is resistant against known-plaintext attacks due to the shifting steps used in the algorithm. It is also resistant to chosen-plaintext attacks, if the H-S-X



(a) (b) (c) (d)

Figure 2.19: (a) Original color image of 'Pepper', (b) Corresponding encrypted image by original Hill cipher cryptosystem, (c) Corresponding encrypted image by proposed H-S-X algorithm, and (d) Corresponding decrypted image by proposed H-S-X cryptosystem.

steps are repeated which is shown in Figure 2.20. This leads to a gradual avalanche effect and hence thwarts the attacks. It incorporates increased diffusion and confusion. Some security analysis has been performed on the proposed encryption technique which includes statistical (histogram, scattered diagram, correlation coefficient) analysis, differential analysis, and entropy measure. The security analyses for the proposed technique with comparison to the original Hill cipher technique are discussed as follows.



(a)

(b)

Figure 2.20: Comparison of 1-round and 4-rounds of H-S-X technique of Capital 'A' image (4-round destructs the image more)

Statistical Analysis

In order to resist the statistical attacks, the encrypted images should possess certain random properties.

Histogram of Encrypted Image:

In order to appear random, the histograms of the encrypted images should be uniformly distributed in all gray levels. Figure 2.21 shows the histograms of original, encrypted, and decrypted images using proposed H-S-X cryptosystem. We compare the gray histogram of the image before and after encryption to analyze the statistical performance. From the figures, it is clear that the original pixel gray values are concentrated on some value, but the pixel gray values after the encryption are scattered in the entire pixel value space, namely, two images have lower similarity. Clearly, it is difficult to use the statistical performance of the pixel gray value to recover the original image. Thereby, proposed H-S-X cryptosystem has strong ability of resisting statistical attack. Also there is no loss of data in decryption. So the proposed method is applicable to protect both conventional and biometric images during communication and transmission. Figure 2.22 shows the scattered diagram between original and encrypted images, original and decrypted images using the proposed H-S-X cryptosystem. Figure 2.22 (a, c, e) shows that, the points spread throughout the surface, that means weaker correlation occurs between original and encrypted images. Figure 2.22(b, d, f) shows that, all the points are along a line. That means stronger correlation occurs between original and decrypted images.

Correlation of Adjacent Pixels

From the result of Table 2.7, it is observed that the correlation coefficient of the adjacent pixels in the encrypted image is very small, which is close to 0 for the proposed method and original image is almost close to 1. The average correlation coefficient is close to 0 for the proposed H-S-X cryptosystem. But in the original Hill cipher method, it is not happen like that. It clearly be seen that the proposed cryptosystem can destroy the relativity effectively; the proposed image encryption cryptosystem has a strong ability to resist statistical attack.

Figure 2.23, 2.24, and 2.25 shows the correlation distribution of two adjacent pixels for 'Capital A', 'Duck', and 'Signature' images respectively by using the proposed H-S-X cryptosystem. From the contrast diagrams it observed that the correlation between pixels of original image is much larger than the correlation between pixels of encryption image. That means, the adjacent pixels of original image have very strong

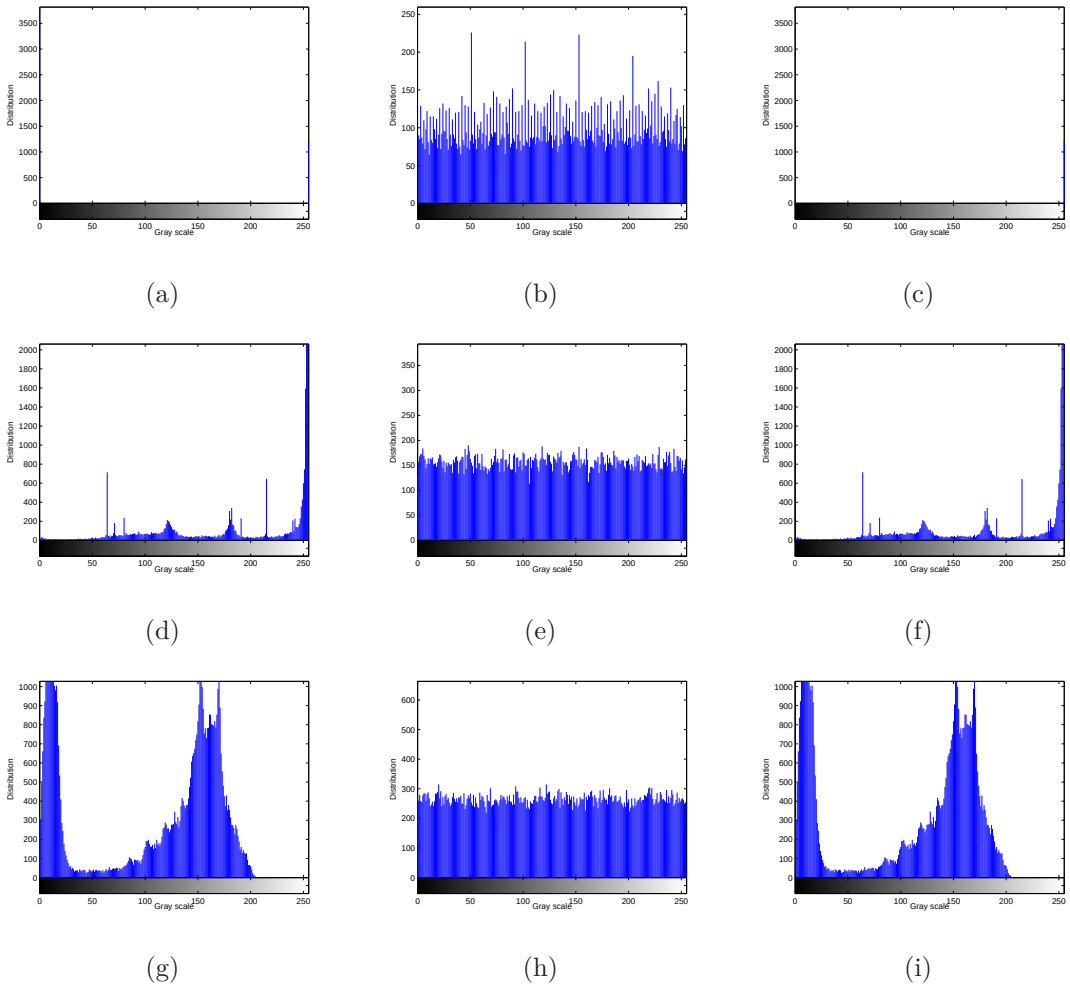


Figure 2.21: (a, d, g) Histograms of original images of 'Capital A', 'Duck', and 'Palmprint' respectively, (b, e, h) Histograms of corresponding encrypted images using the proposed H-S-X cryptosystem, (c, f, i) Histograms of corresponding decrypted images using the proposed H-S-X cryptosystem.

linear correlation, while the correlation between adjacent pixels of encrypted image is very small. It has damaged the linear correlation of original image. Therefore the encrypted algorithm can effectively resist pixel correlation statistical attack.

Differential Analysis

The major requirement of all the encryption techniques is that the encrypted image should be greatly different from its original form. To quantify the difference between encrypted image and corresponding original image, three measures were adopted: Mean Absolute Error (MAE), the Number of Pixel Change Rate (NPCR), and Unified

Table 2.7: Correlation coefficient of the adjacent pixels

Correlation coefficient	Original images				Encrypted images using original Hill cipher				Encrypted images using HSX cryptosystem			
	A	Duck	Palmprint	Pepper	A	Duck	Palmprint	Pepper	A	Duck	Palmprint	Pepper
Horizontal (H)	0.9710	0.9228	0.9959	0.9635	0.6611	0.3547	0.0111	0.0163	0.0063	0.0014	0.0055	0.0019
Vertical (V)	0.9796	0.8959	0.9950	0.9820	0.6294	0.0236	0.0282	0.0234	0.0009	0.0075	0.0034	-0.0030
Diagonal (D)	0.9563	0.8241	0.9928	0.9564	0.5281	- 0.0014	0.0119	0.0165	-0.0020	-0.0021	0.0030	-0.0001
$(H^2 + V^2 + D^2)^{0.5}$	1.6784	1.5275	1.7227	1.6755	1.0545	0.3555	0.0326	0.0329	0.0067	0.0079	0.0071	0.0036
Average (H, V, D)	0.9690	0.8809	0.9946	0.9673	0.6062	0.1256	0.0171	0.0187	0.0017	0.0022	0.0039	-0.0004

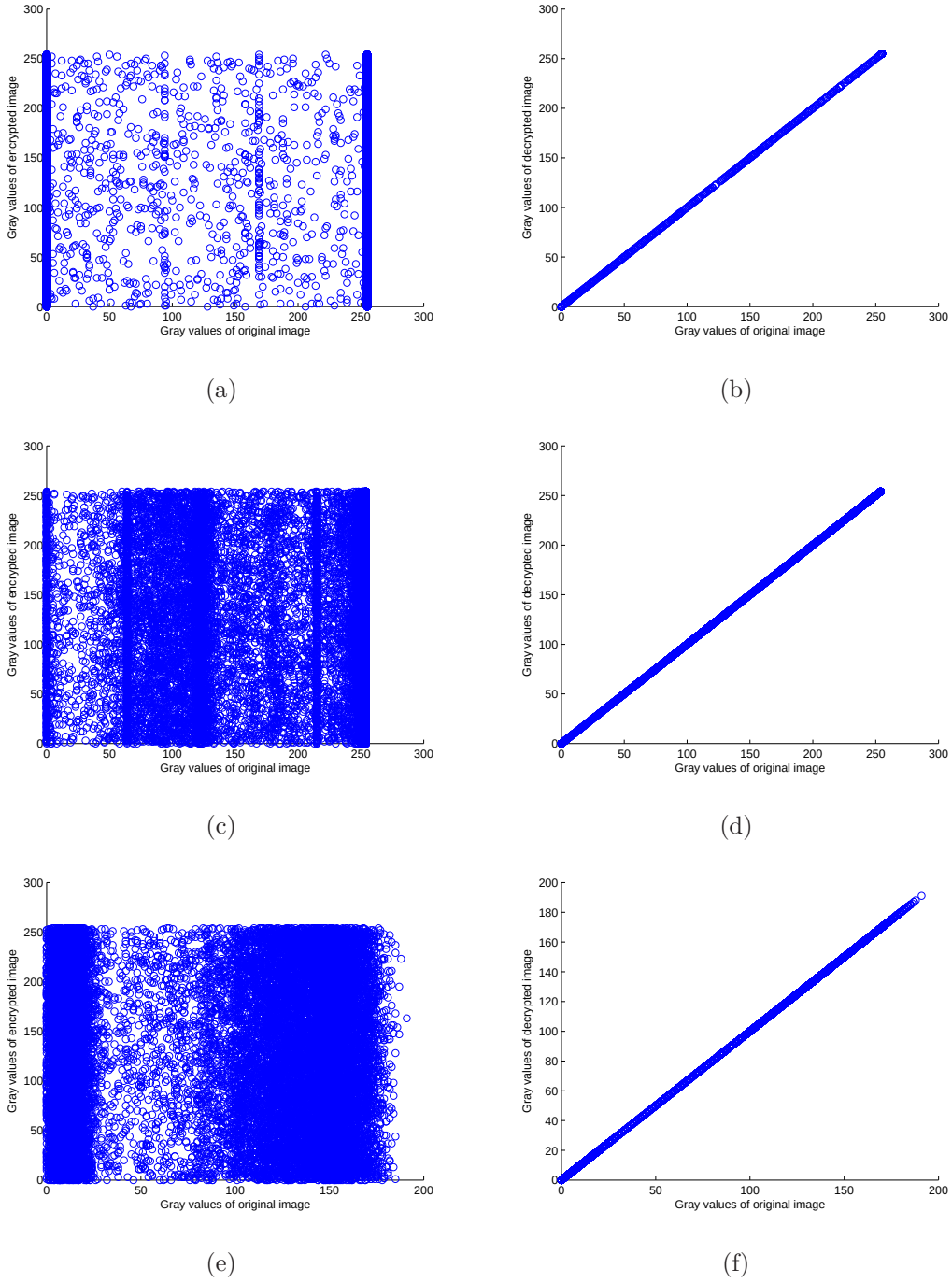
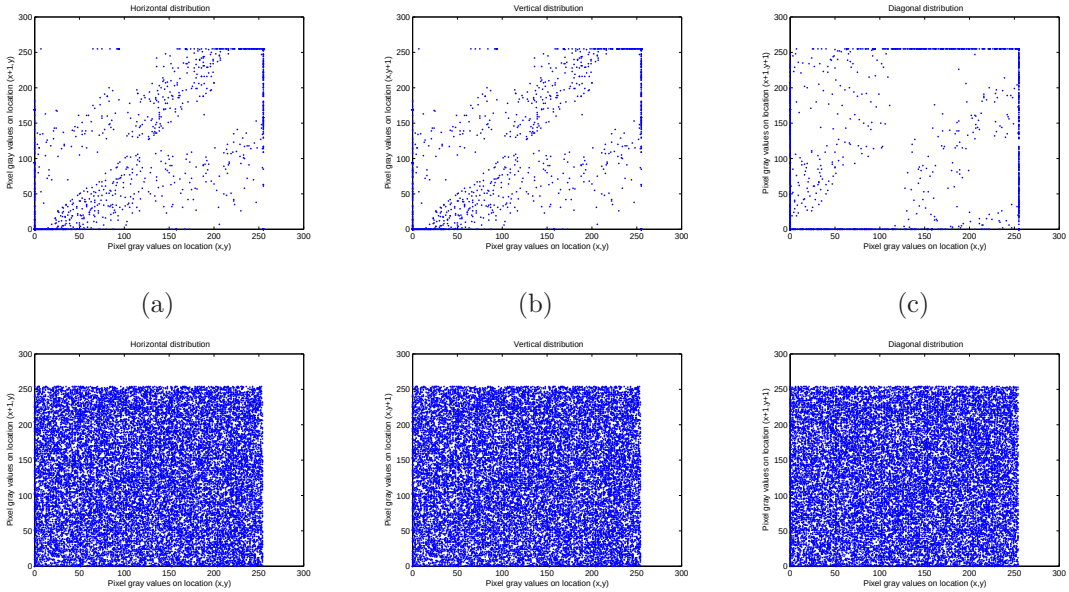


Figure 2.22: (a, c, e) Scattered diagram between original and encrypted images of 'Capital A', 'Duck', and 'Palmprint' respectively using the proposed H-S-X cryptosystem, (b, d, f) Scattered diagram between original and decrypted images of 'Capital A', 'Duck', and 'Palmprint' respectively using the proposed H-S-X cryptosystem.



(a) (b) (c)

(d) (e) (f)

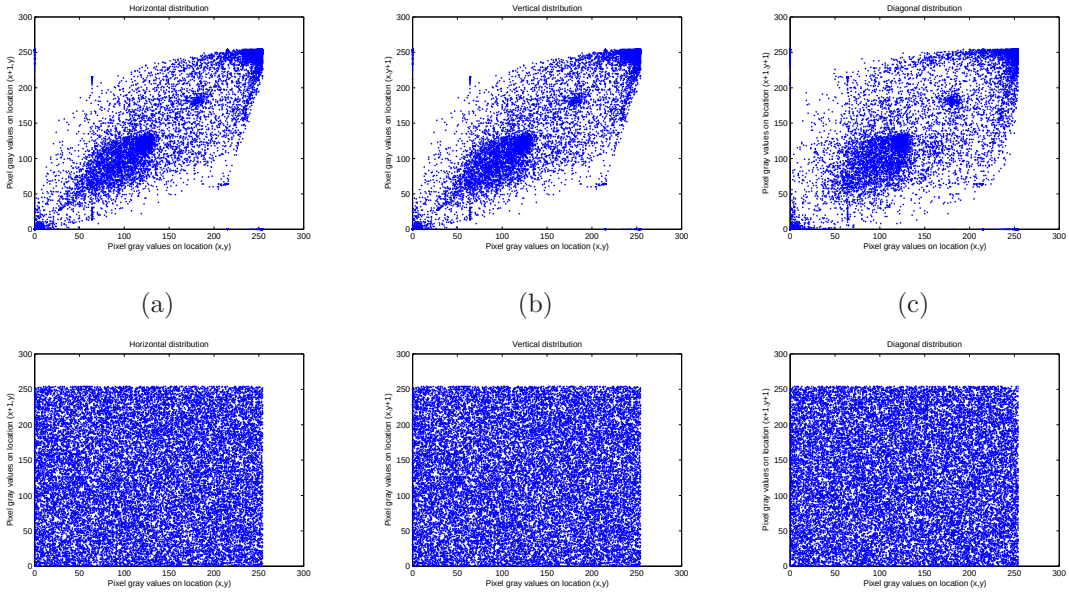
Figure 2.23: Correlation distribution of two adjacent pixels for 'Capital A' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using H-S-X cryptosystem

Average Changing Intensity (UACI). Apart from this PSNR measure is also used to show the efficacy of the proposed method. The analysis shows that, the expected value of NPCR is found to be 99.61%. The expected value of UACI is found to be 33.46%. The larger value of MAE gives better encryption quality. Similarly the smaller value of PSNR gives better encryption quality. The comparison of NPCR, UACI, MAE, and PSNR criteria of various images using the original Hill cipher method and the proposed H-S-X cryptosystem is tabulated in Table 2.8.

The NPCR, UACI, MAE, and PSNR value of proposed H-S-X method is greatly improved as compared to original Hill cipher method. The NPCR and UACI value is also nearer equal or greater than the expected value.

Measure of Entropy

Table 2.9, lists the comparison between entropies of original image and encrypted image using the original Hill cipher algorithm and proposed H-S-X cryptosystem. A higher value of the entropy obtained in case of proposed algorithm as compared to



(a) (b) (c)

(d) (e) (f)

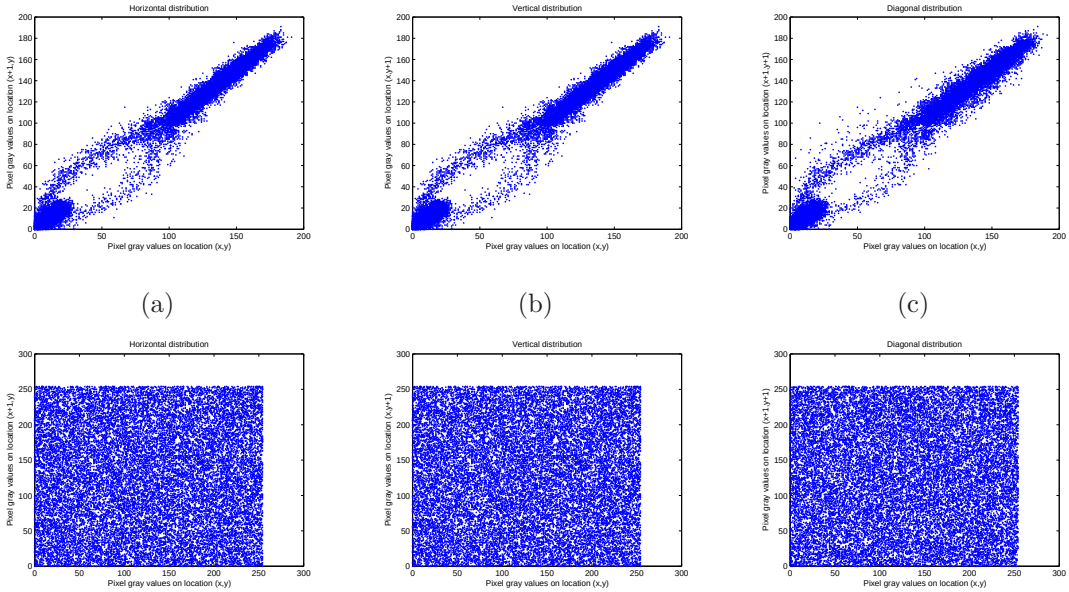
Figure 2.24: Correlation distribution of two adjacent pixels for 'Duck' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using H-S-X cryptosystem

that obtained in the original Hill cipher algorithm indicates that proposed algorithm introduces more randomness in the encrypted image resulting in better encryption.

2.6.4 FPGA Implementation of H-S-X Cryptosystem for Image Encryption

H-S-X algorithm is proposed and it is applied to image encryption application. The algorithm is described in the above sections and this section mainly focuses on FPGA implementation of the same for image encryption. The block diagram for FPGA implementation of H-S-X cryptosystem is shown in Figure 2.26 and from this figure, it is evident that, we need the following for the implementation of H-S-X algorithm in FPGA.

(a) **Hill Cipher Implementation:** Hill cipher implementation is elaborately discussed in FPGA implementation of proposed advanced Hill cipher for image encryption presented in Section 2.5.4.



(a) (b) (c)

(d) (e) (f)

Figure 2.25: Correlation distribution of two adjacent pixels for 'Palmprint' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using H-S-X cryptosystem

(b) **Matrix Adder Architecture:** The matrix adder architecture is customized for row addition. Key will get added to the first row of matrix generated out of two level Hill cipher block. m rows in the key will get added to first row of matrix (output of two-level Hill cipher block) m times. Architecture contains m parallel ($m = 8$) adders placed in m rows. Each row is fed with each row of the key matrix.

(c) **True Random Number Generator (TRNG) :** True random number generator produces a seed for row shifting and column shifting. TRNG produces four bit output. The output of TRNG will get fed into barrel shifters to perform row shifting and column shifting. Basically TRNG is built on Linear Feedback Shift Register (LFSR). Once LFSR enable is on, it starts operation. Once enable signal is pulled off, it stops the operation. Then the output of the LFSR is read into input register of barrel shifter. No seed input required for LFSR, so that it will act like TRNG.

A single bit random number generator produces a value of 0 or 1. The most

Table 2.8: Comparison of NPCR, UACI, MAE, and PSNR criteria of proposed H-S-X cryptosystem and the original Hill cipher algorithm

Criteria (expected value)		Original Image Vs. Encrypted Image	
		Original Hill cipher	Proposed H-S-X cryptosystem
NPCR (99.61%)	A	10.9023	99.2188
	Duck	99.5294	99.6101
	Palmprint	99.5758	99.6429
UACI (33.46%)	A	5.0578	50.1082
	Duck	41.7714	48.5877
	Palmprint	32.4961	32.6486
MAE (Larger Value)	A	12.8974	127.7759
	Duck	106.5171	123.8985
	Palmprint	82.8651	83.2540
PSNR (Smaller Value)	A	14.9358	4.7964
	Duck	6.0079	4.6858
	Palmprint	8.0005	7.9738

efficient implementation is to use a Linear Feedback Shift Register (LFSR). It is based on the recurrence equation:

$$s_n = a_1 * s_{n-1} \oplus a_2 * s_{n-2} \oplus .... \oplus a_m * s_{n-m}$$

Here x_i is the i^{th} number generated, a_i is a pre-determined constant that can be either 0 or 1 and $*$, $\oplus$ are AND, XOR operator respectively. This equation implies that a new number (x_n) can be obtained by utilizing m previous values ($x_{n-1}, x_{n-2}, ..., x_{n-m}$) through a sequence of AND-XOR operations. Figure 2.27 shows the circuit diagram for LFSR based TRNG.

(d) **Barrel Shifters:** Shifting and rotating data is required in several applications including arithmetic operations, variable-length coding, and bit-indexing. Consequently, barrel shifters, which are capable of shifting or rotating data in a single cycle, are commonly found in both digital signal processors and general-purpose processors [44, 45].

Figure 2.28 shows the block diagram for an 8-bit logical barrel shifter, which uses

Table 2.9: Entropy between original image and encrypted image using original Hill cipher and proposed H-S-X cryptosystem

Images	Entropy		
	Original image	Encrypted image	
		Original Hill cipher	Proposed H-S-X cryptosystem
A	1.2256	1.2917	7.9461
Duck	5.2278	7.3058	7.9892
Palmprint	6.9782	7.9836	7.9912

three stages with 4-bit, 2-bit, and 1-bit shifts. A similar unit that performs right rotations, instead of right shifts, can be designed by modifying the connections to the more significant multiplexers. Figure 2.28 also shows the block diagram of an 8-bit right rotator, which uses three stages with 4-bit, 2-bit, and 1-bit rotates. The right rotator and the logical right shifter supply different inputs to the more significant multiplexers. With the rotator, since all of the input bits are routed to the output, there is no longer a need for interconnect lines carrying zeros.

Two barrel shifters are used to shift the pixel values of 8-bits. It is easy to implement MUX based barrel shifter in FPGAs than barrel shifters based on sequential logic. By implementing barrel shifter using multiplexer, we have taken an advantage in area and delay.

Two barrel shifters are used in row shifting block serially to achieve shifting of $m \times m$ $(m = 8)$ matrix. Input bits are fed into barrel shifter parallel. In the similar way, column shifting block is also implemented.

(e) **XOR block for masking:** XOR block consists of series of XOR gates. One input to gate is fed from the output of column shifting barrel shifter and another is fed from the key matrix. This masking will add more security features into image and makes the attack from adversary very difficult.

2.6.5 Results and Discussions

The complete H-S-X algorithm is implemented in Virtex-6 FPGA. All the simulations are done in Virtex 6 ML605 Evaluation Platform, with Xilinx 14.2. The design summary for H-S-X encryption algorithm is shown in Figure 2.29.

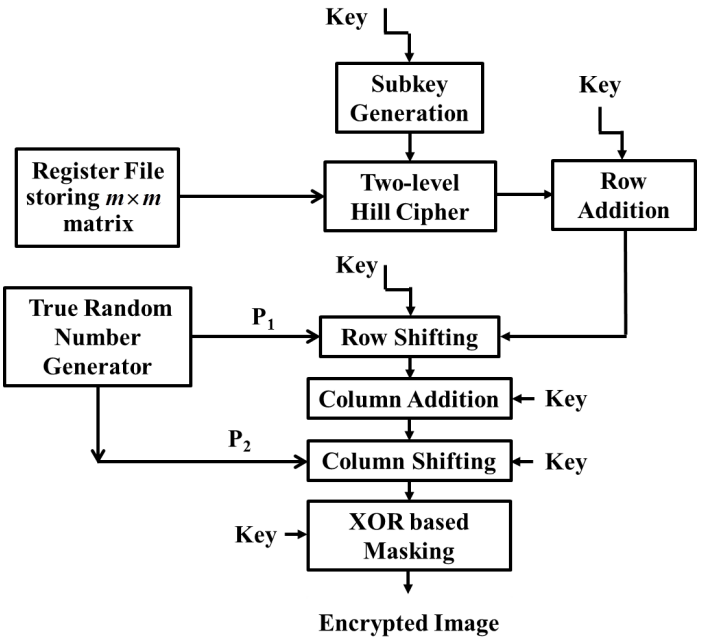


Figure 2.26: Block diagram for FPGA implementation of H-S-X cryptosystem

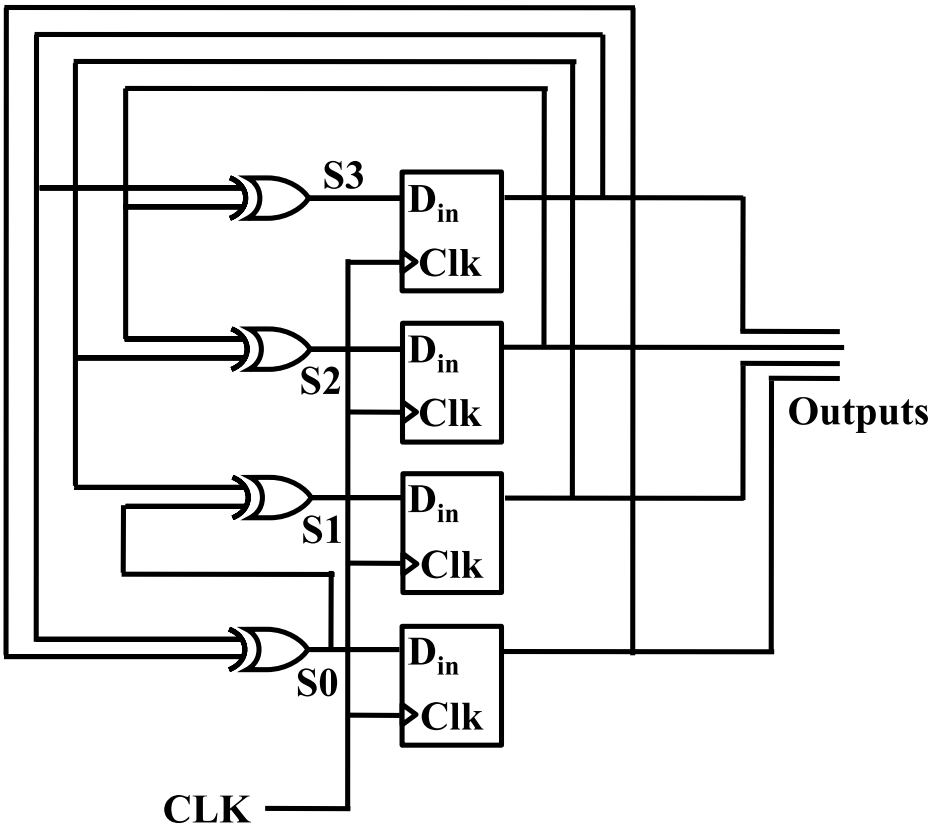


Figure 2.27: Circuit diagram for LFSR based TRNG.

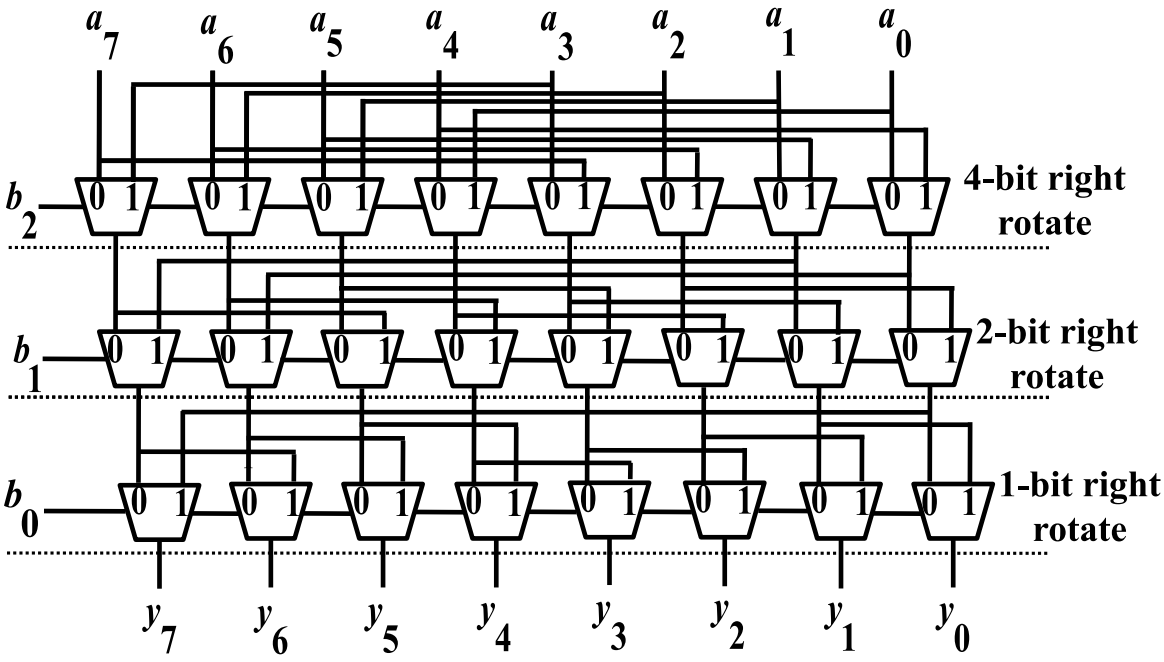


Figure 2.28: 8-bit barrel shifter

hill_cipher_2 Project Status			
Project File:	cipher.xise	**Parser Errors:**	No Errors
Module Name:	hill_cipher_2	**Implementation State:**	Synthesized
Target Device:	xc6vlx240t-1ff1156	• **Errors:**	
Product Version:	ISE 14.2	• **Warnings:**	
Design Goal:	Balanced	• **Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	• **Timing Constraints:**	
Environment:	System Settings	• **Final Timing Score:**	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice LUTs	90	150720	0%
Number of fully used LUT-FF pairs	0	90	0%
Number of bonded IOBs	142	600	23%
Number of DSP48E1s	4	768	0%

Figure 2.29: Design summary for H-S-X encryption algorithm

The design summary for H-S-X decryption algorithm is shown Figure 2.30. The FPGA implementation of H-S-X algorithm is successfully implemented in FPGA Xilinx Virtex-6 FPGA and results are presented.

decipher Project Status			
Project File:	cipher.xise	**Parser Errors:**	No Errors
Module Name:	decipher	**Implementation State:**	Synthesized
Target Device:	xc6vlx240t-1ff1156	**• Errors:**	No Errors
Product Version:	ISE 14.2	**• Warnings:**	6 Warnings (5 new)
Design Goal:	Balanced	**• Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	**• Timing Constraints:**	
Environment:	System Settings	**• Final Timing Score:**	

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice LUTs	96	150720	0%
Number of fully used LUT-FF pairs	0	96	0%
Number of bonded IOBs	143	600	23%
Number of DSP48E1s	4	768	0%

Figure 2.30: Design summary for H-S-X decryption algorithm

2.7 Summary

In this chapter, proposed schemes for invertible, involutory, permutation key matrix generation methods are presented. Subsequently, involutory key matrix generation method applied for image encryption by proposed two algorithms, those are advanced Hill cipher algorithm and H-S-X cryptosystem. The simulation experiments have been conducted in MATLAB and the results have been compared with original Hill cipher to show the efficacy of both the schemes. Both the proposed symmetric cryptosystems (advanced Hill cipher algorithm and H-S-X cryptosystem) can be employed in biometric cryptosystems for encryption of biometric images. Also, in this chapter, advanced Hill cipher algorithm and H-S-X cryptosystem and its FPGA implementation has been performed. Three different methods those are conventional array multiplier, Booth Wallace multiplier and Vedic multiplier are used for FPGA implementation of advanced Hill cipher algorithm. Subsequently comparison has been made with implemented methods in respect to number of multipliers and adders used, number of slices used, maximum combinational path delay and power consumption. Security analysis of both the proposed scheme carried out and compared with the original Hill cipher.

Chapter 3

Conventional and Biometric Image Encryption by Using Extended Hill Cipher Algorithm

Chapter 3

Conventional and Biometric Image Encryption by Using Extended Hill Cipher Algorithm

The basic Hill cipher algorithm can be modified to counter against known plaintext attacks and hence the modified version thus obtained can be used for encrypting bulk amount of text data and image in a secure manner. Sastry et al. [46–52] proposed different modified Hill cipher algorithms. The modification involves like interweaving and iteration, key dependent permutation and circular rotation of the matrix formed by the multiplication of the plaintext matrix P and key matrix K in such a way that known plaintext attack becomes infeasible.

In this chapter, the two schemes of encryption proposed by Sastry et al. [50, 52] which are also called modified Hill cipher involving interweaving and iteration and modified Hill cipher with key dependent permutation and circular rotation are applied for image encryption. Further an extended Hill cipher algorithm based on XOR and zigzag operation for both conventional and biometric image encryption has been proposed. The proposed technique achieves the least encryption and decryption time. Simulation experiments were carried out on standard image using all the three approaches. Following this hybrid cryptosystem is implemented by using RSA algorithm and proposed extended Hill cipher technique to take the advantages of the superior feature of both the techniques.

The rest of this chapter is organized as follows. In Section 3.1, the encryption and decryption algorithm for image encryption using modified Hill cipher with

interweaving and iteration is explained. In Section 3.2, the encryption and decryption algorithm for image encryption using modified Hill cipher with key dependent permutation and circular rotation is presented. Proposed extended Hill cipher algorithm for image encryption is outlined in Section 3.3. In Section 3.4, the basic concept of RSA algorithm is explained. Section 3.5 presents the proposed hybrid cryptosystem and its results. Finally, Section 3.6 summarizes the chapter.

3.1 Image Encryption Using Modified Hill Cipher with Interweaving and Iteration

Sastry et al. [52] developed modified Hill cipher by introducing interweaving (transposition of the binary bits of the plaintext characters belonging to the neighbouring rows and columns) and iteration. In this, the multiplication of the plaintext with the key matrix, the interweaving and the iteration cause a lot of diffusion and confusion. Here, a strong block cipher is developed, whose key length is significantly large.

3.1.1 Encryption and Decryption Algorithm

Consider a plaintext P of $2n$ characters. By using the ASCII code, let us represent P in the form of a matrix, given by

$$P = [P_{ij}],\ i = 1\ to\ n,\ j = 1\ to\ 2. \tag{3.1}$$

Let $K = [K_{ij}]$, $i = 1$ to n, $j = 1$ to n, be the key matrix, in which all the elements are less than 128.

Encryption Algorithm

1. Read $n,\ N,\ K,\ P$.
2. Put $P^0 = P$.
3. Then, interweave the resulting matrix in a column wise and a row wise manner by the following equation:

$$P^i =< KP^{i-1}\ mod\ 128 >,\ i = 1\ to\ N \tag{3.2}$$

where P^i is the resultant matrix for each iteration. Here, $< >$ denotes the interweaving process of the resulting matrix and N denotes the number of times of the interweaving operation.

4. Finally, the ciphertext is obtained by the following equation

$$C = KP^N \ mod\ 128 \tag{3.3}$$

where C is the ciphertext.

Decryption Algorithm

1. Read $n,\ N,\ K,\ C$.
2. Find modular arithmetic inverse of key matrix K, i.e. K^{-1}.
3. Generate

$$P^N = K^{-1}C \ mod\ 128. \tag{3.4}$$

4. Then, reverse process of interweaving is done by the following equation

$$P^{i-1} => K^{-1}P^i \ mod\ 128 <,\ i = N\ to\ 1 \tag{3.5}$$

In this, $><$ denotes the reverse process of interweaving.

5. Finally, the plaintext is obtained by the following equation

$$P = P^0. \tag{3.6}$$

3.2 Image Encryption Using Modified Hill Cipher with Key Dependent Permutation and Circular Rotation

Sastry et al. [50] developed a cipher which involves different types of transformations such as permutation and circular rotation in addition to matrix multiplication and modular arithmetic. This work uses iteration in order to enhance the strength of the cipher.

3.2.1 Encryption and Decryption Algorithm

Consider a plaintext P. It can be represented in the form of a matrix given by

$$P = [P_{ij}],\ i = 1\ to\ n,\ j = 1\ to\ n. \tag{3.7}$$

Consider the key matrix K where

$$K = [K_{ij}],\ i = 1\ to\ n,\ j = 1\ to\ n \tag{3.8}$$

Assume each element in the key matrix between 0 and 127. And let $C = [C_{ij}]$, $i = 1$ to n, $j = 1$ to n be the ciphertext which can be obtained from the plaintext by applying a set of transformations. In order to facilitate this analysis, the above matrices are represented in terms of their corresponding vectors p, k and c given by:

$p = [p_1, p_2, p_3, \ldots, p_{n^2}]$,
$k = [k_1, k_2, k_3, \ldots, k_{n^2}]$, *and*
$c = [c_1, c_2, c_3, \ldots, c_{n^2}]$

While writing these vectors the elements of the corresponding matrices are arranged in a row wise manner.

Encryption Algorithm

1. Read $p,\ k,\ K,\ n,\ r$.

2. Perform the function Permute(p)
   (Permute(p) permutes the binary bits of a plaintext vector in accordance with the numbers present in the key vector.)

3. Perform the function Lrotate(p).
   (Lrotate(p) performs the process of left circular rotation.)

4. Conversion of plaintext vector p into a two dimensional matrix is achieved by the following function

$$P = Convert(p), i = 1\ to\ r \tag{3.9}$$

5. Generate

$$P = KP\ mod\ 128, i = 1\ to\ r \tag{3.10}$$

6. Perform the reverse process of conversion by the following function

$$p = Iconvert(P), i = 1 \; to \; r \tag{3.11}$$

7. Again perform the function

$$Permute(p), \; for \; i = 1 \; to \; r. \tag{3.12}$$

8. Also perform the function

$$Lrotate(p), \; for \; i = 1 \; to \; r. \tag{3.13}$$

9. Then perform the following functions

$$Permute(p) \tag{3.14}$$

$$Lrotate(p) \tag{3.15}$$

10. Finally, the ciphertext is obtained by the following equation

$$c = p \tag{3.16}$$

Decryption Algorithm

1. Read $c, \; k, \; K, \; n, \; r$.

2. Find K^{-1} the modular arithmetic inverse of key matrix K.

3. Put $p = c$.

4. Perform the function Rrotate(p).
   (Rrotate(p) performs the process of right circular rotation.)

5. Perform the function Ipermute(p).
   (Ipermute(p) performs the reverse process of the permute function.)

6. Perform the process of right circular rotation by the function

$$Rrotate(p), \; for \; i = 1 \; to \; r \tag{3.17}$$

7. Perform the function

$$Ipermute(p), \; for \; i = 1 \; to \; r. \tag{3.18}$$

8. Then convert the vector p into a two dimensional matrix by the following function

$$P = Convert(p), i = 1 \; to \; r \tag{3.19}$$

9. Generate

$$P = K^{-1}P \; mod \; 128, i = 1 \; to \; r \tag{3.20}$$

10. Perform the reverse process of conversion by the following function

$$p = Iconvert(P), i = 1 \; to \; r \tag{3.21}$$

11. Then perform the following functions

$$\begin{gathered} Rrotate(p) \\ Ipermute(p) \end{gathered} \tag{3.22}$$

12. Finally, recover the plaintext p.

3.3 Proposed Extended Hill Cipher Algorithm for Image Encryption

The proposed extended Hill cipher algorithm can be used to encrypt a standard image which can also be biometric image stored inside the database of a biometric system. This can ensure the security of template in case of an unauthorized breach to database and to enhance the security of biometric template image during transmission. The proposed extended Hill cipher is more resistant to brute force and known plaintext attacks. This algorithm can also be used to encrypt text.

3.3.1 Encryption and Decryption Algorithm

Consider a plaintext P. Let it can be represented in the form of a matrix given by

$$P = [P_{ij}], 1 \leq i, j \leq n \tag{3.23}$$

and consider the key matrix K where

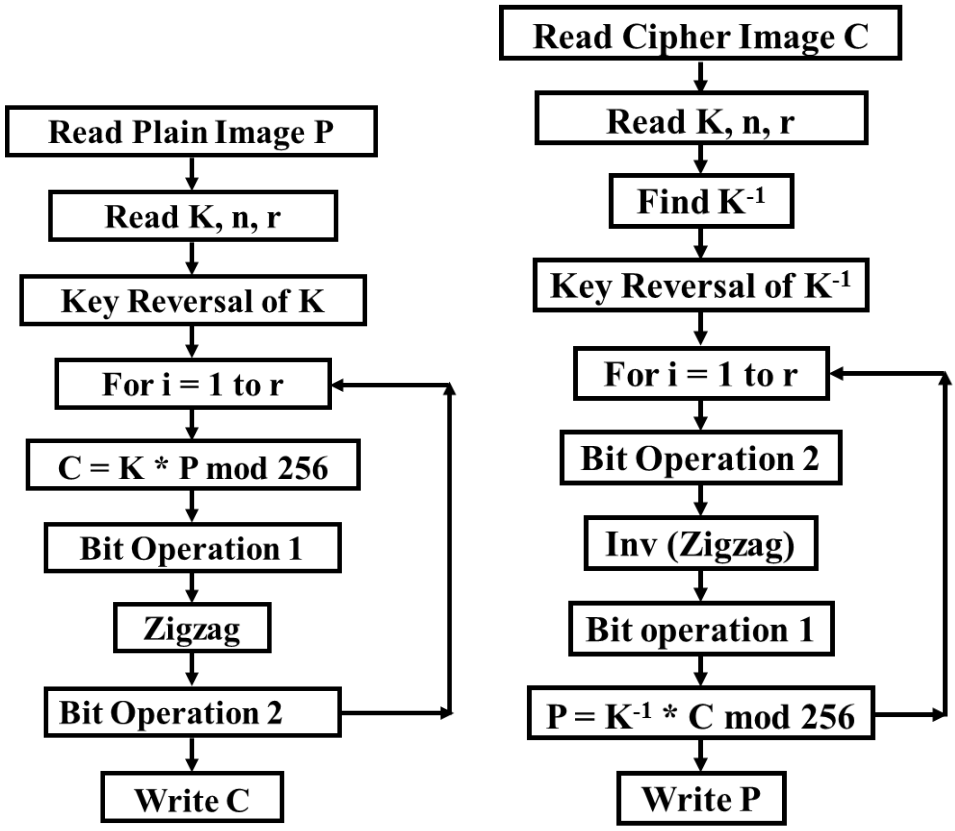
$$K = [K_{ij}], 1 \leq i, j \leq n \tag{3.24}$$

where n is an integer.

Let each element in the key matrix remain between 0 and 255.

Let us assume $C = [C_{ij}]$, $1 \leq i, j \leq n$ be the ciphertext which can be obtained from the plaintext by applying a set of transformations.

The procedures for encryption and decryption of this cipher are shown in Figure 3.1.



(a) Encryption (b) Decryption

Figure 3.1: Block diagram for encryption and decryption using the proposed extended Hill cipher algorithm

Encryption Algorithm

1. Read plain image or text P, key matrix K, n and r, where n is an integer and r denotes the number of iterations.

2. Perform the key binarization and key reversal operation of the key matrix K. In this the elements of the key matrix K are represented in terms of 8-bit binary equivalent and saved as binary equivalent key matrix k.

Then perform the reversal operation of the binary equivalent key matrix k as

$$kk = seqrevrese(k) \tag{3.25}$$

3. Now the process of iteration starts for $i = 1$ to r.
   At first, the key matrix K is multiplied with the plain image or text matrix P to form an intermediate cipher matrix C, represented by the equation

$$C = K * P \ mod \ 256 \tag{3.26}$$

4. Secondly, perform XOR-bit operation-1 on the cipher image or text C with the key matrix k for $i = 1$ to r.
   For this first convert the cipher image or text C into its binary equivalent matrix c. Then perform logical-XOR operation with the key matrix k to form the resultant cipher matrix $c1$. That means,

$$c1 = xor(k, c) \tag{3.27}$$

5. Thirdly, perform zigzag operation on the cipher matrix $c1$.
   In this the rows of the matrix $c1$ are rotated as per the assumed key vector of the user to form the resultant cipher matrix $c2$.

6. Perform XOR-bit operation-2 on the cipher matrix $c2$ with the reversal key matrix kk for $i = 1$ to r to form the cipher matrix $c3$. That means,

$$c3 = xor(c2, kk) \tag{3.28}$$

   Repeat step-3 to step-6 for r times. The process of iteration ends here.

7. Finally, recover the cipher image or text C.

Decryption Algorithm

1. Read cipher image or text C, key matrix K, n and r.
   where n is an integer and r denotes the number of iterations.

2. Find modular arithmetic inverse of key matrix K, i.e. K^{-1}.

3. Perform the key binarization and key reversal operation of the inverse key matrix.

The elements of the inverse key matrix are represented in terms of their 8-bit binary equivalent and saved as binary equivalent key matrix k.
Then perform the reversal operation of the binary equivalent key matrix k as

$$kk = seqrevrese(k) \tag{3.29}$$

4. Now the process of iteration starts for $i = 1$ to r.
   At first, perform XOR-bit operation-2 on the cipher matrix c with the reversal key matrix kk for $i = 1$ to r, forming of the resulted cipher matrix $c1$. That means,
   $$c1 = xor(c, kk) \tag{3.30}$$
   For that first convert the cipher image or text C into its binary equivalent matrix c. Then after perform logical-XOR operation with the reversal key matrix kk.

5. Secondly, perform inverse zigzag operation on the cipher matrix $c1$, forming of the cipher matrix $c2$.

6. Thirdly, perform XOR-bit operation-1 on the resulted cipher matrix $c2$ with the key matrix k for $i = 1$ to r, forming of the resulted cipher matrix $c3$. That means,
   $$c3 = xor(c2, k) \tag{3.31}$$

7. Inverse of key matrix K is multiplied with the cipher image or text matrix $C3$ to form plain image or text matrix P, represented by the equation
   $$p = K^{-1} * C3 \ mod \ 256 \tag{3.32}$$
   Repeat step-4 to step-7 for r times. The process of iteration ends here.

8. Finally, recover the plain image or text P.

3.3.2 Simulation Results

Encryption and decryption of 'Lena' image by using modified Hill cipher with interweaving and iteration [52], modified Hill cipher with key dependent permutation and circular rotation [50], and proposed extended Hill cipher algorithm are performed. Results are shown in Figure 3.2. In Figure 3.2(f), it is observed that there are few data loss during decryption in modified Hill cipher with key dependent permutation and circular rotation method. But at the same time in the proposed extended Hill

cipher method and modified Hill cipher with interweaving and iteration method there are no loss of data during decryption.

Figure 3.2: (a, d, g) Original 'Lena' images, (b, c) Encrypted and decrypted results of 'Lena' image using modified Hill cipher with interweaving and iteration, (e, f) Encrypted and decrypted results of 'Lena' image using modified Hill cipher with key dependent permutation and circular rotation, and (h, i) Encrypted and decrypted results of 'Lena' image using proposed extended Hill cipher method respectively.

3.3.3 Security Analysis and Discussion

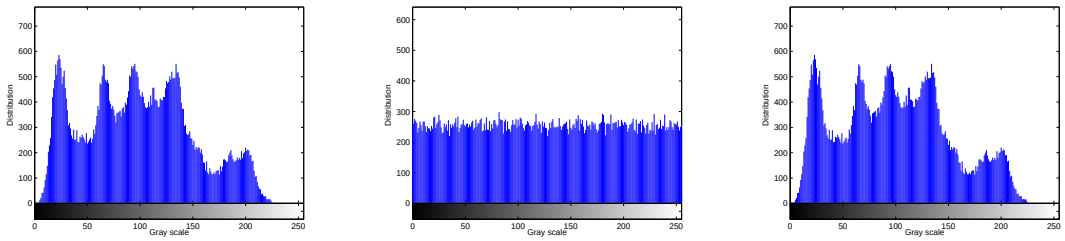
Security analysis has been carried out on the proposed extended Hill cipher technique which includes statistical (histogram, scattered diagram, correlation coefficient), differential analysis, and entropy measure in comparison to other techniques.

Statistical Analysis

In order to resist the statistical attacks, the encrypted images should possess certain random properties.

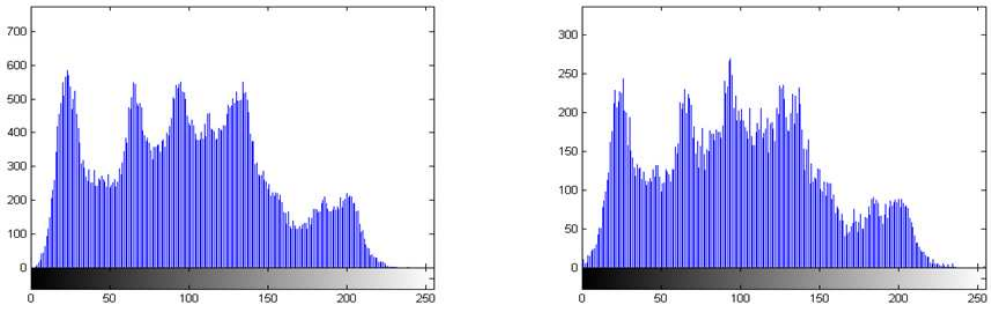
Histogram of Encrypted Image

In order to appear random, the histograms of the encrypted images should be uniformly distributed in all gray levels. Figure 3.3 shows the histograms of plain 'Lena' image and their encrypted and decrypted results using proposed extended Hill cipher algorithm. It is observed that histogram of encrypted image is wide and uniform throughout the dynamic range of the image as a result gives high quality of encryption. The proposed method has no data lost during decryption, so our algorithm has strong ability of resisting statistical attack. So the proposed method is applicable to protect both conventional and biometric images during communication and transmission. Figure 3.4 shows the histogram of original 'Lena' image and histogram of corresponding decrypted image using modified Hill cipher with key dependent permutation and circular rotation. Statistical analysis of original and decrypted image histogram and also from the decrypted image matrix it is observed that few variations are there because of some data loss occurred in decrypted image. Figure 3.5 shows the scattered diagram between original and encrypted images, original and decrypted images using modified Hill cipher with interweaving and iteration, modified Hill cipher with key dependent permutation and circular rotation, and proposed extended Hill cipher method. In Figure 3.5(e), it shows that, the points are spread throughout the surface as compared to other two methods. That means weaker correlation occurs between original and encrypted image in the proposed system. In Figure 3.5(f), it observed that, all the points are along a line as compared to other two methods. That means stronger correlation occurs between original and decrypted image in the proposed system.



(a) (b) (c)

Figure 3.3: (a) Histogram of original 'Lena' image, (b) Histogram of corresponding encrypted image using proposed extended Hill cipher method, (c) Histogram of corresponding decrypted image using proposed extended Hill cipher method.



(a) (b)

Figure 3.4: (a) Histogram of original 'Lena, image, (b) Histogram of corresponding decrypted image using modified Hill cipher with key dependent permutation and circular rotation.

Correlation of adjacent pixels

From Table 3.1, it is observed that the correlation coefficient of the adjacent pixels in the encrypted image is very small, which is close to 0 for the proposed method and original image is almost close to 1. The average correlation coefficient is close to 0 for the proposed method. It clearly be seen that the proposed algorithm can destroy the relativity effectively; the proposed image encryption algorithm has a strong ability to resist statistical attack. From the contrast diagrams of Figure 3.6 it can be observed that the correlation between pixels of original image is much larger than the correlation between pixels of encryption image, that means the adjacent pixels of original image have very strong linear correlation, while the correlation between adjacent pixels of encrypted image is very small. It has damaged the linear correlation of original image.

Therefore the proposed encrypted algorithm can effectively resist pixel correlation statistical attack.

Table 3.1: Correlation coefficient of the adjacent pixels for 'Lena' image

Correlation coefficient	Original image	Modified Hill cipher using interweaving and iteration	Modified Hill cipher using key dependent permutation and circular rotation	Proposed extended Hill cipher
Horizontal (H)	0.9384	-0.0225	0.3495	-0.0017
Vertical (V)	0.9698	0.0757	0.2588	0.0126
Diagonal (D)	0.9164	-0.0222	0.0864	-0.0006
$(H^2 + V^2 + D^2)^{0.5}$	1.6313	0.0820	0.4433	0.0127
Average (H, V, D)	0.9415	0.0103	0.2316	0.0034

Differential Analysis

To quantify the difference between encrypted image and corresponding plain-image, three measures were adopted: Mean Absolute Error (MAE), the Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). The comparison of NPCR, UACI, and MAE criteria of various images using the proposed extended Hill cipher algorithm, modified Hill cipher with interweaving and iteration, and modified Hill cipher with key dependent permutation and circular rotation is shown in Table 3.2. Also in this table, PSNR value is presented to show the efficiency of the methods. Apart from this, encryption and decryption time are also compared with the other two methods, which is as shown in Table 3.3.

From Table 3.2, it reveals that the NPCR value is approximately equal to the expected value and the NPCR value of the proposed method is higher than the other two methods. The UACI value is also nearer equal to the expected value and the

Table 3.2: Comparison of NPCR, UACI, MAE, and PSNR criteria of proposed extendeded Hill cipher algorithm and others.

Criteria (expected value)	Original Image Vs. Encrypted Image		
	Modified Hill cipher with interweaving and iteration	Modified Hill cipher with key dependent permutation and circular rotation	Proposed extended Hill cipher
NPCR (99.61%)	99.4095	99.5560	99.6031
UACI (33.46%)	19.0226	23.3807	30.6471
MAE (Larger value)	48.5075	52.6209	78.1502
PSNR (Smaller value)	12.6618	10.9068	8.5514

Table 3.3: Comparison of encryption time and decryption time criteria of proposed extended Hill cipher algorithm and others.

Sl. No.	Parameters	Modified Hill cipher with interweaving and iteration	Modified Hill cipher with key dependent permutation and circular rotation	Proposed extended Hill cipher algorithm
1	Encryption Time	4.15 sec	6.35 sec	1.20 sec
2	Decryption Time	3.07 sec	6.45 sec	1.50 sec

Table 3.4: Entropy between original 'Lena' image and encrypted image using modified Hill cipher with interweaving and iteration, modified Hill cipher with key dependent permutation and circular rotation, and proposed extended Hill cipher method

Images	Entropy			
	Original Image	Encrypted Image		
		Modified Hill cipher with interweaving and iteration	Modified Hill cipher with key dependent permutation and circular rotation	Proposed extended Hill cipher method
Lena	7.5977	7.8972	7.4327	7.9565

UACI value of the proposed method is higher than the other two methods. The MAE value is larger in the proposed method and also larger than the other two methods. The PSNR value of the proposed method is smaller than the other two methods. Table 3.3 shows that the proposed algorithm is faster than the other two methods. Simulation are carried out by Matlab R2010b, computation platform is Windows Vista with Intel(R) Core(TM)2 Duo, CPU 2.00 GHz and EMS memory is 3.00 GB.

Measure of Entropy

The comparison of the entropy between original image and encrypted image using the modified Hill cipher with interweaving and iteration, modified Hill cipher with key dependent permutation and circular rotation, and the proposed extended Hill cipher method are presented in Table 3.4. A higher value of the entropy obtained in case of proposed algorithm indicates more randomness in the encrypted image as compared to other two methods resulting in better encryption.

Avalanche Effect

The proposed extended Hill cipher algorithm has been verified for avalanche effect and it follows this strictly. Both confusion and diffusion are found in accordance with the

avalanche effect. Proposed algorithm extended Hill cipher algorithm is also suitable for encryption of text messages. In this section plaintext is applied to proposed algorithm to verify the avalanche effect by changing few inputs.

Let a plaintext P and key K is coded as

P=[137 136 133 136; 137 136 133 136; 138 133 134 134; 133 133 133 130]

K=[4 3 5 4; 2 4 5 3; 1 2 3 5; 6 5 0 6];

Then the ciphertext C is coded as

C=[159 80 241 225; 62 241 73 244; 9 173 56 130; 90 250 49 148];

Now if K(9)=8 and P(9)=68 then the corresponding cipher is

C=[211 123 1 126; 62 241 152 244; 9 173 191 130; 90 250 72 148];

From the above example it shows that, the corresponding cipher has changed from the previous cipher and thus it follows avalanche effect.

Safe Time

A cipher is more resistant to intruder attack if it has significant time for detection of the key matrix. A original image of size 256×256, is taken for encryption in the proposed method and the safe time is calculated by the following formula

$$T_{safe} = \tfrac{1}{2}(N^{m \times m} \times T)$$

where N is the base size of plaintext or image, m is the size of the key and T is the time for one trial.

In the proposed algorithm, $N = 256$, let $m = 8$, and $T = 0.075$ second. Therefore, $T_{safe} = 5.02 \times 10^{152}$ seconds, which is a very long time to find the key matrix.

3.4 RSA Algorithm

RSA is an algorithm for public-key cryptography. The RSA algorithm was publicly described in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT (Massachusetts Institute of Technology) [78]. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n for some n. A typical size for n is 1024 bits. That is, n is less than 2^{1024}. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $log(n)$; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$.

The RSA algorithm involves three steps: key generation, encryption and decryption.

3.4.1 Key Generation Algorithm:

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated in the following way:

1. Choose two distinct random prime numbers p and q of similar bit-length.
2. Compute the key length, $n = pq$ where n is used as the modulus for both the public and private keys.
3. Compute the function: $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p+q-1)$.
4. Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$ that means e and $\varphi(n)$ share no divisors other than 1 i.e. e and $\varphi(n)$ are coprime. Here, e is the public key exponent.
5. Determine d (using modular arithmetic) as $d \equiv e^{-1}(mod\ \varphi(n))$; where d is the multiplicative inverse of $e(modulo\ \varphi(n))$ (using modular arithmetic) which satisfies the congruence relation.

$$d.e \equiv 1(mod\ \varphi(n)) \tag{3.33}$$

   This is often computed using the extended Euclidean algorithm. d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

3.4.2 Encryption Algorithm

1. Consider the plaintext block be M and ciphertext block be C. For encryption, first turns M into an integer m, such that $0 \leq m < n$ by using padding scheme.

2. Then computes the ciphertext c corresponds t

$$c \equiv m^e \ (mod\ n) \tag{3.34}$$

Sender transmits that ciphertext c to the receiver.

3.4.3 Decryption Algorithm

1. Receiver recover m from c by using her private key exponent d, which is as follows:

$$m \equiv c^d \ (mod\ n) \tag{3.35}$$

2. Then receiver recovers the original message M from m by reversing the padding scheme.

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PU = \{d, n\}$.

This algorithm to be satisfactory, the following requirements must be met:

a. It is possible to find values of e, d, n such that $m^{ed}\ mod\ n = m$ for all $m < n$.

b. It is relatively easy to calculate $m^e\ (mod\ n)$ and $c^d\ (mod\ n)$ for all values of $m < n$.

c. It is infeasible to determine d given e and n.

d. The first relationship $m^{ed}(mod\, n) = m$ holds if e and d are multiplicative inverses modulo $\varphi(n)$, where $\varphi(n)$ is the Euler totient function.

3.4.4 Advantages of RSA

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his

signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems.

3. Data block length is more.

4. Ciphering and deciphering keys are different.

5. Ciphering and deciphering algorithms are same.

3.5 Proposed Hybrid Cryptosystem

Cryptosystems are divided into the symmetric or secret key cryptosystem and asymmetric or the public key cryptosystem depending on the key used. The symmetric cryptosystem are faster, simple and efficient but it is disadvantageous in the way that the key distribution process needs to be completed. On the other hand, the public key cryptosystem is advantageous in the way that the key distribution process is not necessary because the key used for encryption can be made public by placing it in a public directory. However, it is less efficient than the symmetric cryptosystem since it takes much time for encryption/decryption. Thus, raised the need for a cryptosystem which combines the advantages of both the symmetric and the public key cryptosystem [79, 100]. Here hybrid cryptosystem implemented, hybrid cryptosystem where RSA algorithm has been used as the asymmetric cryptosystem to encrypt the symmetric key to solve the problem of key distribution. Proposed modified Hill cipher which gives high quality of encryption is used to encrypt the information. Both the cryptosystems were combined to form a hybrid cryptosystem. The block diagram of proposed hybrid cryptosystem is shown in Figure 3.7.

3.5.1 Encryption and Decryption Algorithm

The algorithm for proposed cryptosystem are presented as below.

1. The image is taken and encrypted by using the proposed extended Hill cipher algorithm and symmetric encryption key $K1$.

2. The symmetric key $K1$ is encrypted by using RSA algorithm with the help of public key $K2$.

3. Then the encrypted key $K1$ and the encrypted image are transmitted to the receiver side.

4. On the receiver side, the encrypted key is decrypted by using the RSA decryption algorithm with the help of private key $K3$.

5. Then the cipher image is decrypted by using the decrypted key and the proposed extended Hill cipher algorithm.

3.5.2 Simulation Results and Discussion

Image encryption and decryption with proposed symmetric cryptosystem that is extended Hill cipher algorithm is employed in hybrid cryptosystem and it is already described in Section 3.3. This hybrid cryptosystem can also be utilized to transfer messages safely and in this section we present the results of a sample message encryption and decryption. The simulation is performed with GNU Octave. Figure 3.8 and 3.9 shows the encryption and decryption of the message using hybrid cryptosystem respectively.

For the input message ”NITRAIPUR", the encrypted text is ”RK’KPNMRUFHE[EhSPD”. The symetric key is also encrypted with public key of RSA. The decryption yields the original message.

3.6 Summary

The two encryption schemes such as modified Hill cipher involving interweaving and iteration and modified Hill cipher with key dependent permutation and circular rotation are applied for image encryption. Further an extended Hill cipher algorithm based on XOR and zigzag operation for both conventional and biometric image encryption has been proposed. The proposed technique achieves the least encryption and decryption time. Simulation experiments and security analysis were carried out for all the three approaches and compared. Following this hybrid cryptosystem is implemented by using RSA algorithm and proposed extended Hill cipher technique to take the advantages of the superior feature of both the techniques. The algorithms developed for both the techniques are simulated using MATLAB and GNU Octave.

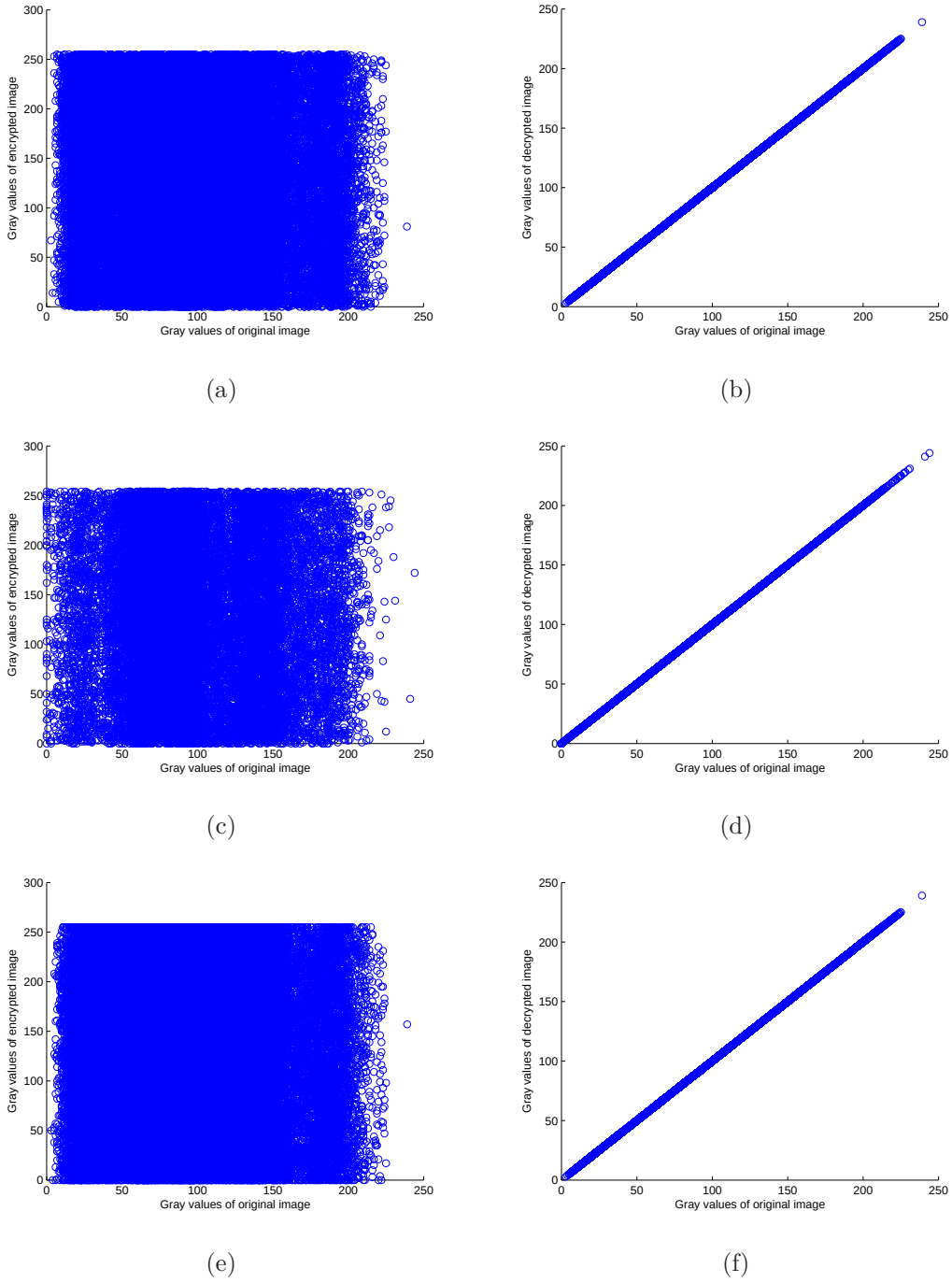


Figure 3.5: (a, c, e) Scattered diagram between original and encrypted images of 'Lena' using modified Hill cipher with interweaving and iteration method, modified Hill cipher with key dependent permutation and circular rotation method, and proposed extended Hill cipher method respectively, (b, d, f) Scattered diagram between original and decrypted images of 'Lena' using the corresponding three methods respectively.

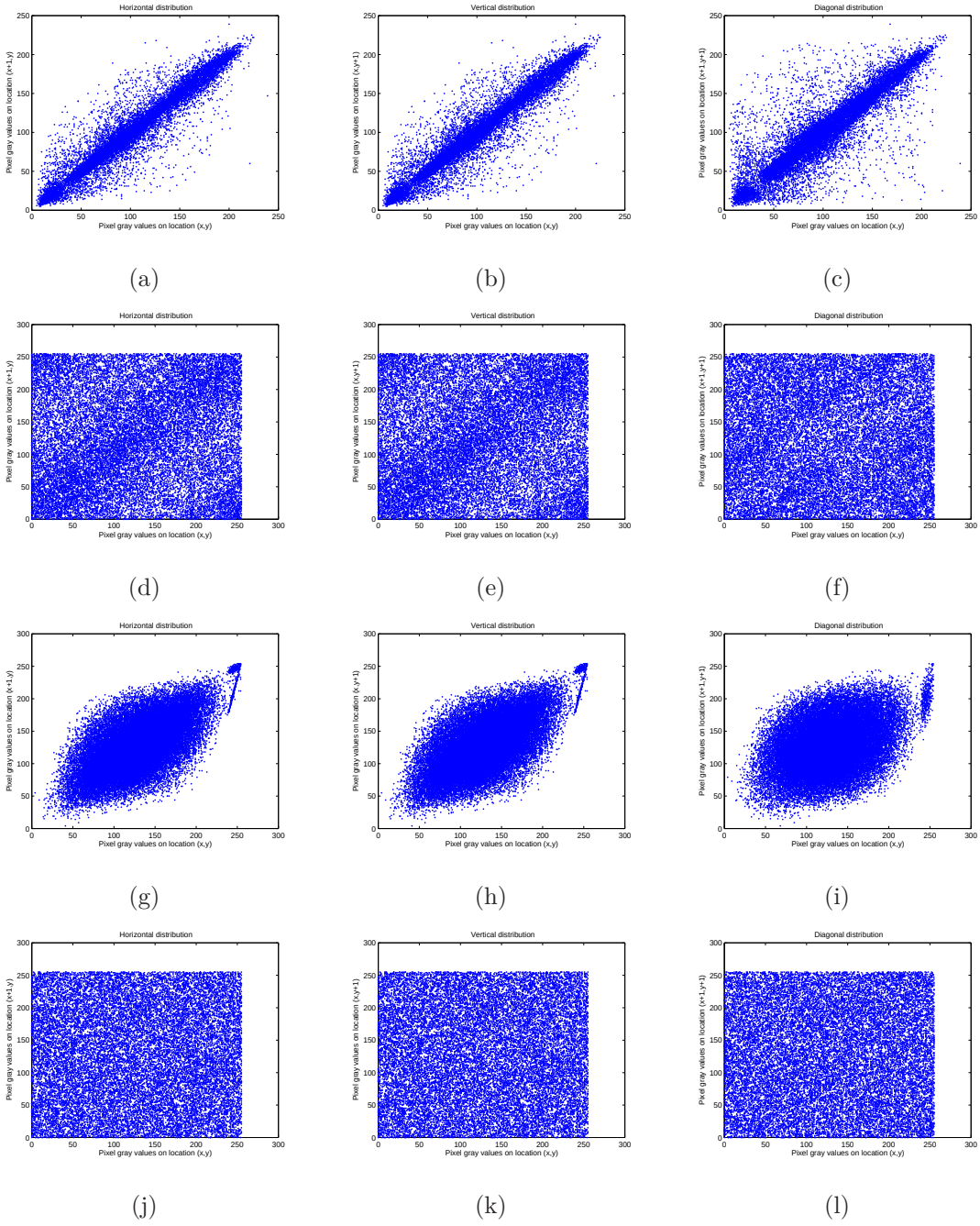


Figure 3.6: Correlation distribution of two adjacent pixels for 'Lena' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f), (g, h, i) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted 'Lena' image using modified Hill cipher with interweaving and iteration method and using modified Hill cipher with key dependent permutation and circular rotation method respectively, and (j, k, l) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted 'Lena' image using proposed extended Hill cipher method.

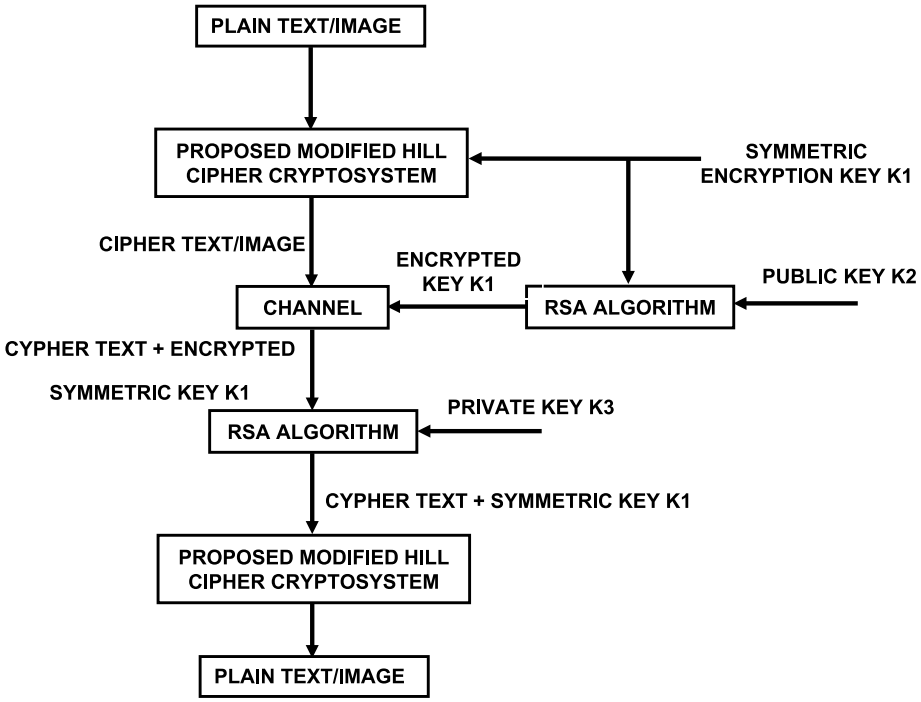


Figure 3.7: Block diagram of hybrid cryptosystem

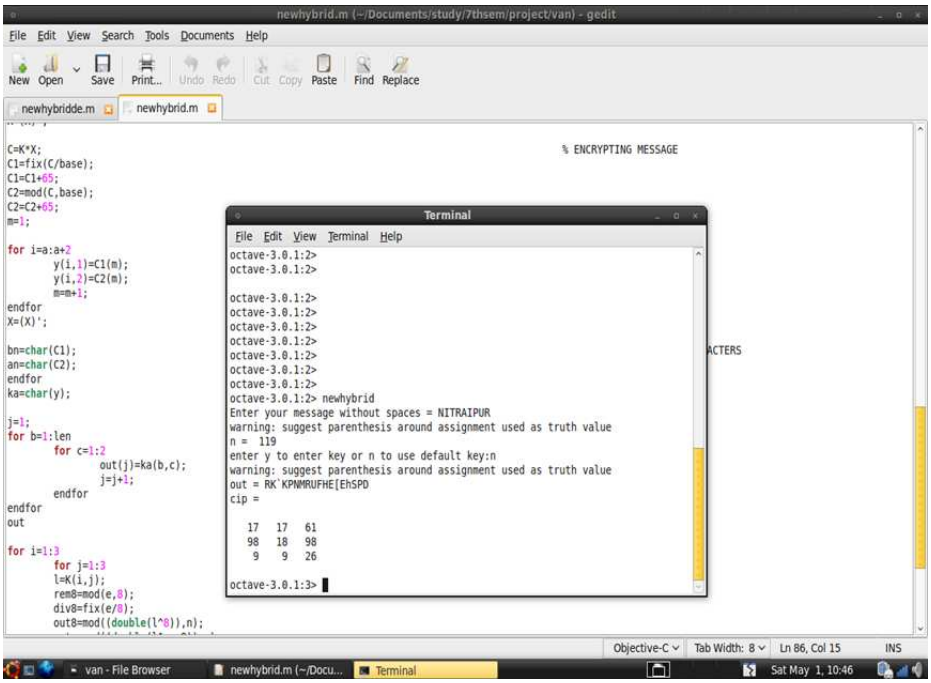


Figure 3.8: Encryption using hybrid cryptosystem

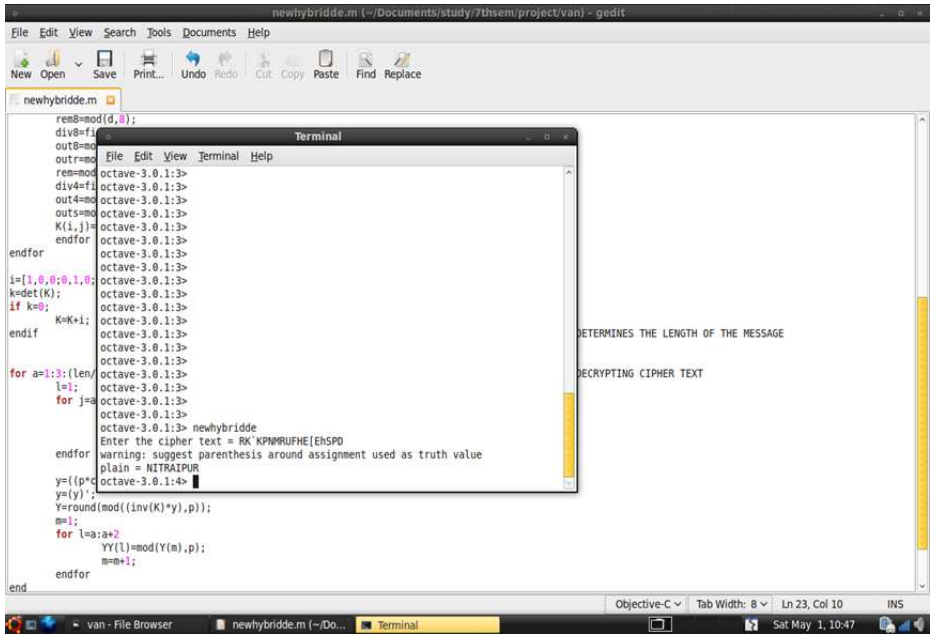


Figure 3.9: Decryption using hybrid cryptosystem

Chapter 4

Development of Novel Multilevel Image Encryption Scheme

Chapter 4

Development of Novel Multilevel Image Encryption Scheme

With the fast development of computer and network technologies, the security of image data has become inevitable. Due to some intrinsic features of images, traditional encryption schemes such as DES, IDEA, and AES etc. are not very suitable for image encryption [71]. Chaos based cryptosystem, achieves an excellent level of image encryption and many contributions have been devoted to the methods of using chaos to construct digital cipher since 1989 [74]. In general, the term 'chaos' refers to a situation or place of great disorder and unpredictability. However, researches have shown that image encryption algorithms based only on chaotic maps, such as one-dimensional chaotic maps, multi-dimensional chaotic maps and ultra-dimensional chaotic maps have lower key space and are liable to be interpreted [6].

Recent research has considered DNA as a medium for ultra-scale computation and for ultra-compact information storage. One potential key application is DNA-based, molecular cryptography systems [67]. DNA cryptography is a technique in which DNA is used as an information carrier and the modern biological technology is used as an implementation tool. The vast parallelism, exceptional energy efficiency and extraordinary information density inherent in DNA molecules are used in cryptography such as encryption, authentication, signature, etc. [6]. In recent years, many DNA based chaotic encryption techniques have been put forward [68–75].

Poker Shuffling [7] based image scrambling method which is controlled dynamically by chaotic system. It is a method of shuffling the pixel to increase the correlation coefficient between adjacent pixels. This shuffling helps increasing the security level of the encrypted image. Compared with other scrambling techniques such as algebraic

permutations [8] and chaotic permutations [9–11], it has properties of nonlinearity, large key space and non-analytic formula. In addition, its scrambling performance is satisfied and can deal with non-square image. All these features show that the poker shuffling is more secure and efficient for image scrambling encryption [7].

In the present chapter, at first image encryption and decryption using chaos based DNA coding along with shifting and scrambling operation algorithm is presented. Secondly proposed algorithm of image encryption and decryption using chaos based DNA coding along with poker shuffle operation is presented. Then this chapter exemplifies resultant analysis and comparison of both the methods based on NPCR, UACI, MAE, PSNR and entropy. Finally FPGA implementation [101, 102] of image encryption and decryption using chaos based DNA coding along with shifting and scrambling operation is presented.

The rest of this chapter is organized as follows. The basic concept of chaos theory, DNA coding and poker shuffling theory is presented in Section 4.1, 4.2, and 4.3 respectively. In Section 4.4, algorithm for image encryption and decryption based on chaos, DNA coding along with shifting and scrambling operation has been outlined. Proposed algorithm for image encryption and decryption using chaos based DNA coding along with poker shuffle operation is presented in Section 4.5. Simulation results are presented in Section 4.6. Security analysis and discussion are presented in Section 4.7. In Section 4.8 FPGA implementation of image encryption and decryption based on chaos, DNA coding along with shifting and scrambling operation is presented. Finally, summary are provided in Section 4.9.

4.1 Chaos Theory

Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions; an effect which is popularly referred to as the butterfly effect. Differences in initial conditions such as those due to rounding errors in numerical computation yield widely diverging outcomes for chaotic systems, rendering long-term prediction unfeasible in general. This happens even though these systems are deterministic, i.e. their future behavior is fully determined by their initial conditions, without involving random elements. The deterministic nature of these systems does not make them predictable.

Although there is no universally accepted mathematical definition of chaos, a commonly used definition says that, for a dynamical system to be classified as chaotic,

it must have the following properties:

- It must be sensitive to initial conditions;
- It must satisfy topologically mixing; and
- Its periodic orbits must be dense.

4.1.1 Chaotic Maps

In order to make the process of image encryption more efficient, most scholars sights on the field of chaos. A chaotic map is a map (evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or a continuous-time. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems. Because of the properties of chaos theory, researchers have adopted different types of chaotic maps to put image in disorder. The type of chaotic map used in this work is logistic map.

Logistic Map

One of the simplest and most widely studied nonlinear dynamical systems capable of exhibiting chaos is the logistic map.

$$F(x, r) = rx(1 - x) \tag{4.1}$$

Or written in its recursive form,

$$x_{n+1} = rx_n(1 - x_n),\ 0 \leq x_n \leq 1,\ 0 \leq r \leq 4 \tag{4.2}$$

Here, F is the transformation mapping function, r is the bifurcation parameter which determines the map behavior and n is the iteration number that discretizes time. Depending on the value of r, the dynamics of this system can change attractively, exhibiting periodicity or chaos.

The bifurcation diagram is shown in Figure 4.1. The bifurcation parameter r is shown on the horizontal axis of the plot and the vertical axis shows the set of values of the logistic function visited asymptotically from almost all initial conditions. Figure 4.1 shows the forking of the periods of stable orbits from 1 to 2 to 4 to 8 etc. Each of these bifurcation points is a period-doubling bifurcation.

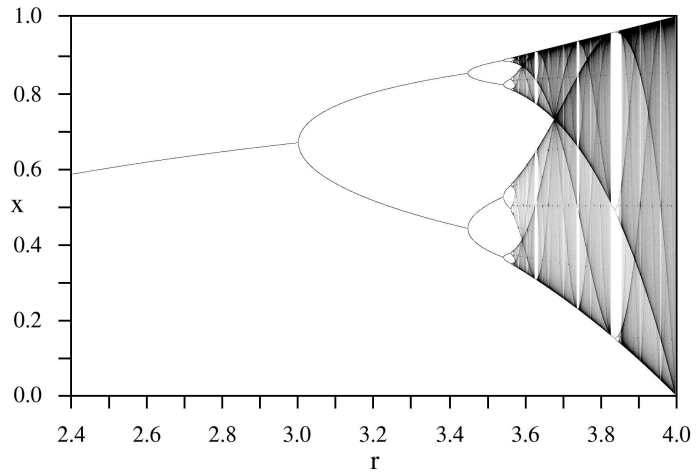


Figure 4.1: Bifurcation diagram of the logistic map

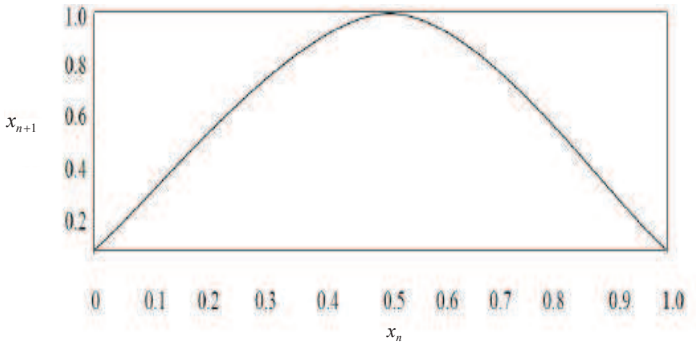


Figure 4.2: Graph of the logistic function $x_{n+1} = rx_n(1 - x_n)$ for one dimension and $r = 1$

The first bifurcation occurs at $r = 3$, leading to a stable period-2 cycle which eventually lose stability, as $r \ll 3.45$, giving rise to a stable period-4 cycle. As r increases further, the scenario repeats itself over and over again: each time a period-2 k cycle of the map F loses stability through a bifurcation of the map F, which gives rise to initially stable period-2 cycle, where F is often mentioned logistic map with a periodic point of prime period k.

For $0 < r < r_c = 3.57$, the sequence $\{x_n\}$ of values of r at which cycles of period $2k$ appear has a finite accumulation point $r \ll 3.57$. For $r_c < r < 4$, the sequence is, for all practical purposes, non-periodic and non-converging. The resultant sequence will be chaotic sequence.

Further, a very interesting and useful feature of chaotic maps is their sensitivity to the initial value x_0, any small disturbance in the value of x_0 results in completely

different output sequence. Simultaneously, it is mathematically shown that, except for negligibly short intervals where the sequence has odd periodicities, this particular range of values of r causes the logistic map to be chaotic over $\{0, 1\}$.

Figure 4.2 can be used to show that the logistic map is also chaotic by geometry of the iterated map and restricted to $\{0, 1\}$ value at $r = 1$. However, further investigation provides that map has indeed, a period-2 cycle for r slightly greater than three, equivalently, or fixed point is depicted in this figure.

4.2 DNA Coding Theory

In 1994, Dr Adleman [66] released "Molecular Computation of Solutions to Combinatorial Problems" in Science, which indicated a new research field-DNA computing. DNA computing is a new method that uses biological molecule DNA as computing medium and biochemical reaction as computing tools. DNA computing uses DNA molecules of the double helix structure of special and complementary base pair coding information laws, to be put into operation by the image of the target DNA coding sequence of DNA designed to molecular chain, on the role of enzymes in biology, the generation of data pool, and then the rules must be in accordance with the original image into a problem of computing a high degree of parallel DNA molecular chain of the controlled sublimation of the reaction process, and finally detected by the use of molecular biology required for computing the results [68].

The basic elements of DNA are nucleotide, because of the different chemical structure, nucleotide are divided into four basic alphabets: Adenine (A), Guanine (G), Cystosine (C) and Thymine (T) as shown in Figure 4.3. Owing to the key hydrogen, the two chains are put together, and form a double helix structure chain, and that one chain in the base sequence complementary to the other, that is A and T are pairs, G and C are pairs [68].

Four base pairs composed of a collection of letters, that is,

$$\text{Set} = \{\text{C, A, T, and G}\}$$

DNA molecule has structure to save enormous data and perform massive parallel reaction.

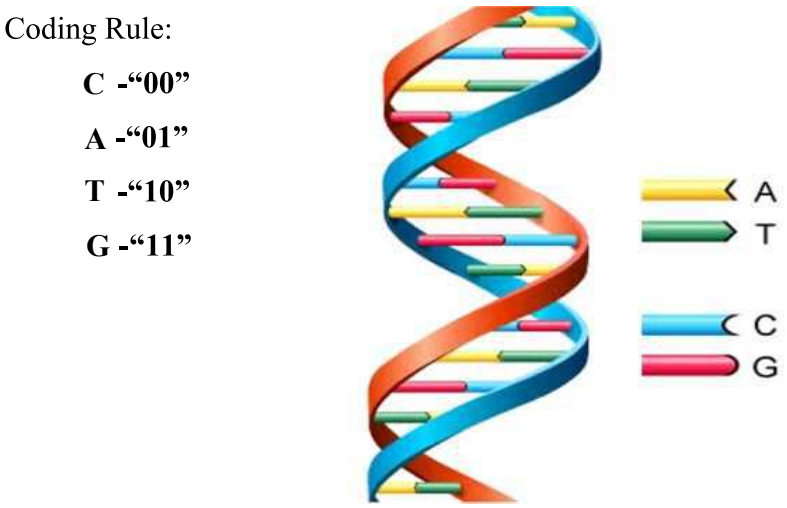


Figure 4.3: DNA strand

4.3 Poker Shuffling Theory

The history of poker is thought to have evolved over more than ten centuries from various games, all involving the basic principles of ranked card or domino combinations. The standard poker game has flourished not only in all kinds of nongovernmental gambling but also the formal cosmopolitan bridge matches. As one of key factors of poker game, the card shuffle techniques have also evolved for very long time to make the permutation of each card fully random and unpredicted so that the fairness and credibility of game are guaranteed. This implies that the poker shuffle has great randomness and indetermination.

Image scrambling is an important technique in digital image encryption and digital image watermarking. Since image scrambling is essentially to rearrange all the pixels over plain image, poker shuffling is an image scrambling method which is controlled dynamically by chaotic system and can be used to achieve high security [7].

4.4 Image Encryption and Decryption based on Chaos, DNA Coding along with Shifting and Scrambling

In this section image encryption and decryption algorithm based on chaos, DNA coding along with shifting and scrambling are presented.

4.4.1 Algorithm for Image Encryption

1. Take an original input image and convert it into gray image matrix, which is expressed as $A(m, n)$, where m, n is row and column of the image.

2. Now convert this two-dimensional gray image matrix elements (0-255) into binary numbers (00000000-11111111), forming of binary image matrix.

3. Applying DNA code rule ($C = 00, A = 01, T = 10, G = 11$) and encode the binary image matrix by taking 2 bits at a time. DNA encoded matrix PP of size $(m, n * 4)$ is generated.

4. Generate the chaotic sequence by logistic map using 2 groups of different initial values x and $x1$.

5. Now generate a chaotic matrix '$x2'$, where $x2 = x * x1^T$.

6. A chaotic binary matrix QQ is generated by thresholding the matrix '$x2'$.

7. Then applying DNA rule, to generate a chaotic DNA matrix $QQ1$.

8. Now generate a matrix RR by adding two matrices PP and $QQ1$ using the DNA add rule which is shown in Figure 4.4.

ADD	A	T	C	G
A	A	T	C	G
T	T	C	G	A
C	C	G	A	T
G	G	A	T	C

Figure 4.4: DNA add rule

9. Again generate two chaotic sequence 'p' and 'q'.

10. Then generate a chaotic matrix 'z', where $z = p * q^T$.

11. Now again thresholding the chaotic matrix to generate a chaotic binary matrix SS.

12. After that, generate the complemented matrix CC, which is as follows: If the elements of the binary chaotic matrix SS is 1, then the corresponding elements in the matrix RR is complemented otherwise no change occurs in the matrix RR.

13. Now decoding that means binarization of the CC matrix, to generate $CC1$ matrix by using the DNA rule as before and then reconstruct to an image matrix.

14. Perform shifting and scramble operation on the image matrix, to generate an encrypted image E.

4.4.2 Algorithm for Image Decryption

The decryption process is the reverse process of encryption.

1. The encrypted image matrix is expressed as $E(m, n)$, where m, n is row and column of the image.

2. The encrypted image is first descrambled.

3. This descrambled image is then vertically de-shifted, then horizontally de-shifted.

4. Then convert this two-dimensional matrix element (0-255) into binary numbers (00000000 -11111111), then by using DNA encoding rules ($C = 00, A = 01, T = 10, G = 11$), encode this binary numbers by 'C, A, T, G', forming of the matrix PP of size $(m, n * 4)$.

5. Generate the chaotic sequence by logistic map using 2 groups of different initial values 'm' and 'n'.

6. Generate a chaotic matrix 'y', where $y = m * n^T$.

7. Now the chaotic binary matrix KK is generated using thresholding the chaotic matrix 'y'.

8. Generate a chaotic DNA matrix $KK1$ applying DNA rule.

9. Generate the matrix AA by subtracting the chaotic DNA matrix image $KK1$ from the image DNA matrix PP by using DNA subtraction rule which is as shown in Figure 4.5.

SUB	A	T	C	G
A	A	G	C	T
T	T	A	G	C
C	C	T	A	G
G	G	C	T	A

Figure 4.5: DNA substract rule

10. Again generate two chaotic sequence 'u' and 'v'.
11. Then generate a chaotic matrix 'w', where $w = u * v^T$.
12. Thresholding the chaotic matrix to generate a chaotic binary matrix BB.
13. Generate the complemented matrix GG, in following process: If the elements of the binary chaotic matrix BB is 1, then the corresponding elements in the matrix AA is complemented otherwise no change is made in the matrix AA.
14. Now decoding that means binarization of the AA matrix, to generate $AA1$ matrix by using the DNA rule as before and then reconstruct to an image matrix.

The encryption scheme based on chaos, DNA coding along with shifting and scrambling operation is shown in Figure 4.6.

4.5 Algorithm for Image Encryption and Decryption based on Chaos, DNA Coding along with Poker Shuffle

The algorithm presented in Section 4.4 is for image encryption and decryption based on chaos, DNA coding along with shifting and scrambling operation. In this proposed algorithm, shifting and scrambling operation is replaced with poker shuffle to gain advantages. This proposed method with poker shuffle has properties of nonlinearity, non-analytic formula and large key space. Moreover its scrambling performance is

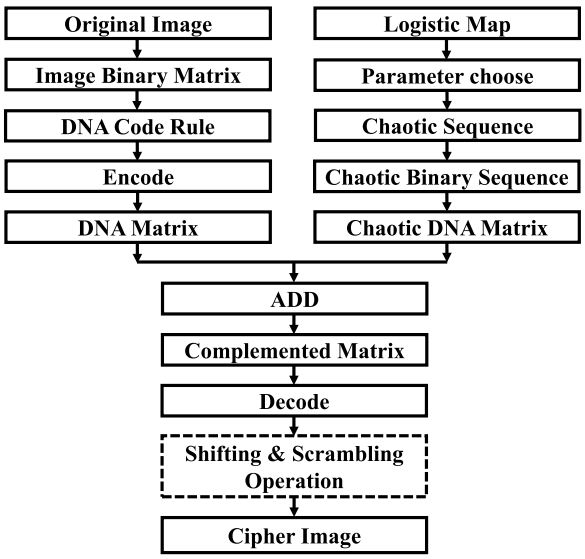


Figure 4.6: Block diagram for image encryption based on chaos, DNA coding along with shifting and scrambling operation

satisfied and can deal with non-square images. These features of poker shuffling shows that it is more secure and efficient for image scrambling encryption. Poker shuffle operations and its image scrambling algorithm proposed by Wang et al. [7] is described in following section.

4.5.1 Poker Shuffle Operations

Basically, poker shuffle is composed of three operations: card intercrossing, card extracting and card cutting. Without loss of generality, the initial sequence is assumed to be arranged by its nature order, i.e. $sq = 1, 2, 3, \ldots, L$. Here we assume $sq = 1, 2, 3, \ldots, 11$ to demonstrate the shuffle operations.

Card intercrossing operation $S_{sq}(p_1, q_1)$

Firstly, split sequence $sq = (1, 2, 3, \ldots, 11)$ into two subsequences $sq_1 = (1, 2, \ldots, 5)$ and $sq_2 = (6, 7, \ldots, 11)$, then repeat intercrossing sq_1 and sq_2 with interval p_1 for q_1 times to get the new sequence sq' . If the number of remaining elements is less than p_1, then directly intercross the remaining part. For example, after performing $S_{sq}(2, 1)$ operation on sq, we will get the new sequence

$$sq' = (6, 7, 1, 2, 8, 9, 3, 4, 10, 11, 5)$$

If operation is $S_{sq}(2,2)$ the resultant sequence is,

$$sq' = (9,3,6,7,4,10,1,2,11,5,8)$$

Card extracting operation $D_{sq}(p_2, q_2)$

Extract subsequence from original sequence $sq = (1,2,\ldots,p_2-1,p_2,\ldots,q_2,q_2+1,\ldots,11)$ where the subsequence is indexed from p_2 to q_2, and then put the subsequence at the begin of sq. After completing this operation, we get the new sequence $sq' = (p_2,\ldots,q_2,1,\ldots,p_2-1,q_2+1,\ldots,11)$. Note that p_2, q_2 should be exchanged if $p_2 > q_2$.

For example, $sq' = D_{sq}(4,7) = (4,5,6,7,1,2,3,8,9,10,11)$.

Card cutting operation $T_{sq}(p_3)$

Select subsequence from original sequence $sq = (1,2,\ldots,p_3-1,p_3,p_3+1,\ldots,11)$, where the subsequence is indexed from p_3 to the end of sq, and then move it to the begin of sq. After that, the result sequence is $sq' = (p_3,\ldots,11,1,\ldots,p_3-1)$.

For example, $sq' = T_{sq}(4) = (4,5,6,7,8,9,10,11,1,2,3)$.

Obviously, $D_{sq}(p_2,q_2)$ is identical with $T_{sq}(p_3)$ if $q_2 = 11$ or $p_2 = 11$, thus $T_{sq}(p_3)$ is the special case of $D_{sq}(p_2,q_2)$.

To improve the randomness of poker shuffle, chaotic systems are suggested. Due to distinct properties of chaotic systems such as randomness, ergodicity, sensitivity dependence on initial conditions and parameters, it is suggested to control the shuffle process. Simply means, from the above three shuffle operations, the values of p_i and q_i is generated by chaotic systems and decide the processing order of q_3.

Consider Tent map be of simple arithmetic and uniform PDF, it is thus employed to accomplish this task. The Tent map is given as:

$$x_{i+1} = F_\alpha(x_i) = \begin{cases} x_i/\alpha, & 0 \le x_i \le \alpha \\ (1-x_i)/(1-\alpha), & \alpha < x_i \le 1 \end{cases} \tag{4.3}$$

where α is control parameter and x_0 is initial value.

Based on Tent map, parameters p_i and q_i are valued as follows: Discard the first $r(r \ge 32)$ iterations and continuing to iterate for 6β times, p_i and q_i are then valued by:

$$
\begin{aligned}
p_1 &= mod\left(\left\lfloor x_\beta * 2^{24} \right\rfloor, 8\right) + 1 \\
q_1 &= mod\left(\left\lfloor x_{2\beta} * 2^{24} \right\rfloor, 4\right) + 1 \\
p_2 &= mod\left(\left\lfloor x_{3\beta} * 2^{24} \right\rfloor, M\right) + 1 \\
q_2 &= mod\left(\left\lfloor x_{4\beta} * 2^{24} \right\rfloor, M\right) + 1 \\
p_3 &= mod\left(\left\lfloor x_{5\beta} * 2^{24} \right\rfloor, M\right) + 1 \\
q_3 &= mod\left(\left\lfloor x_{6\beta} * 2^{24} \right\rfloor, 6\right) + 1
\end{aligned} \tag{4.4}
$$

where, M is the row or column size of image to be scrambled, $\lfloor . \rfloor$ is the floor function, and $K = (\alpha, x_0, r, \beta)$ is used as the secret key for image scrambling. According to the value of q_3, the shuffle operations are ordered correspondingly and the changeable poker shuffle process is listed in Table 4.1. Obviously, the shuffle result has great randomness and is decided completely by secret key K.

Table 4.1: Process of Poker Shuffle decided by q_3

q_3	**Order of shuffle operations**
1	$S_{sq}(p_1, q_1), D_{sq}(p_2, q_2), T_{sq}(p_3)$
2	$D_{sq}(p_2, q_2), T_{sq}(p_3), S_{sq}(p_1, q_1)$
3	$T_{sq}(p_3), S_{sq}(p_1, q_1), D_{sq}(p_2, q_2)$
4	$S_{sq}(p_1, q_1), T_{sq}(p_3), D_{sq}(p_2, q_2)$
5	$D_{sq}(p_2, q_2), S_{sq}(p_1, q_1), T_{sq}(p_3)$
6	$T_{sq}(p_3), D_{sq}(p_2, q_2), S_{sq}(p_1, q_1)$

4.5.2 Image Scrambling Algorithm

Consider an image whose size is $M * N$ and denoted by matrix $P_{i,j}$ $(1 < i < M, 1 < j < N)$. For a given secret key $K = (\alpha, x_0, r, \beta)$ the scrambling algorithm based on poker shuffle is described as follows:

Row scrambling

1. Without loss of generality, let the original row sequence be

$$sq_r = 1, 2, 3, \cdots, M \tag{4.5}$$

2. Generate parameters p_i, q_i and perform the poker shuffle process according to Table 4.1 to get the shuffled row sequence

$$sq_r{}' = \{r_i, i = 1, 2, \cdots\cdots, M\} \tag{4.6}$$

where $r_i \in [1, M]$ and $r_i \neq r_j$ if $i \neq j$

3. Then rearrange the row of matrix $P_{i,j}$ in terms of sq'_r, that is, move the r_1 row to the first row, r_2 row to the second row,...,r_M row to the last row. Thus a row-scrambled matrix $P^r_{i,j}$ is generated, which is shown in the following example.

Let $sq'_r = \{3, 5, 1, 4, 2\}$. The row of matrix $P_{i,j}$ is arranged in terms of sq'_r, forming of row-scrambled matrix $P^r_{i,j}$. So according to sq'_r, the row scrambling is shown in Figure 4.7.

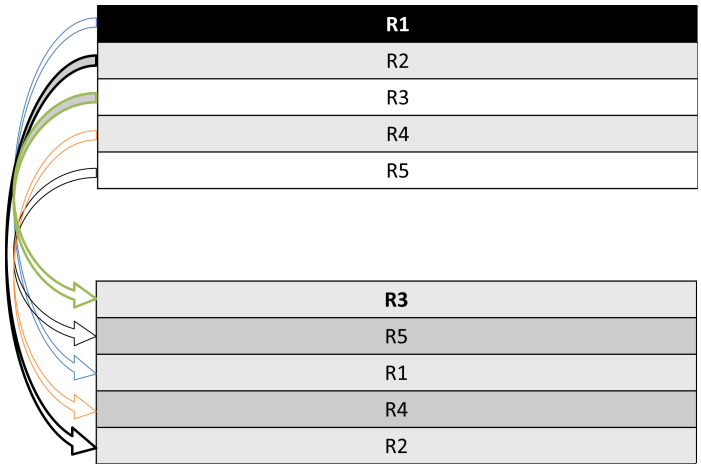


Figure 4.7: Row scrambling operation

Column scrambling

For the new matrix $P^r_{i,j}$, we will produce the column-scrambled matrix column by column. Let the original column sequence be $sq_c = (1, \cdots, N)$, the scrambling process is presented as follows:

1. Using the present $x_{6\beta}$ as initial value x_0 and continue to iterate to generate parameters p_i,q_i. According to the shuffling process of Table 4.1, the resultant shuffle sequence presented as:

$$sq_c{}' = \{c_i, i = 1, 2, \cdots, N\} \tag{4.7}$$

where $c_i \in [1, N]$ and $c_i \neq c_j$ if $i \neq j$

2. Rearrange the position of every column for the first row of matrix $P^r_{i,j}$ according to sq'_c, that is, move the c_1 column to the first column, c_2 column to the second column,...,c_M column to the last column, thus a scrambled column of the first row of matrix $P^r_{i,j}$ is generated.

3. From the second row till the last row of matrix $P^r_{i,j}$, do the same column scrambling in the same way as step 1 and step 2, thus a final scrambled matrix $p^{rc}_{i,j}$ is produced.

   Let $sq'_c = \{3, 5, 1, 4, 2\}$. The columns of each row of the matrix $P^r_{i,j}$ is arranged in terms of sq'_c, forming of final row column-scrambled matrix $p^{rc}_{i,j}$. So according to sq'_c, the column scrambling is shown in the Figure 4.8.

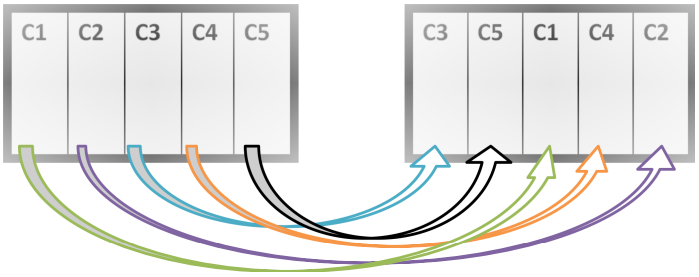


Figure 4.8: Column scrambling operation

For brief, let us assume the described scrambling algorithm is called as A-I. Only column-direction is fully scrambled while row-direction does not in A-I. To improve its confusion performance, it can further use the same mode of column scrambling to replace the row scrambling, so that the pixels are thoroughly scrambled in two directions. Let this thorough scrambling algorithm is called as A-II for convenience. It is obvious that its confusion performance is expected to be much higher than A-I, and so does its security. Of course, its time complexity is almost twice of A-I.

The encryption scheme based on chaos, DNA coding along with poker shuffle operation is shown in Figure 4.9.

4.6 Simulation Results

Different images, either conventional or biometric images are encrypted and decrypted by using proposed chaos based DNA coding along with shifting and scrambling and proposed chaos based DNA coding along with poker shuffling and the results are shown

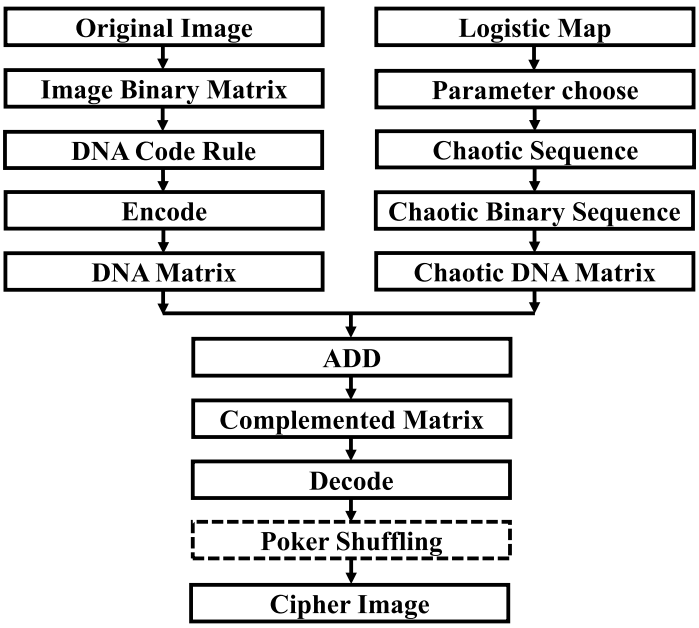


Figure 4.9: Block diagram for image encryption based on chaos, DNA coding along with poker shuffle operation

in Figure 4.10. In Figure 4.10, it is clear that both the proposed methods can able to encrypt the images properly. So the proposed methods are applicable to protect both conventional and biometric images during communication and transmission. The face image is taken from the Yale face database [103].

4.7 Security Analysis and Discussion

Some security analysis has been performed on the proposed encryption techniques which includes statistical (histogram, scattered diagram, correlation coefficient) analysis, differential analysis, and entropy measure. The security analyses for both the proposed chaos based DNA coding along with shifting and scrambling and chaos based DNA coding along with poker shuffling techniques are discussed as follows.

4.7.1 Statistical Analysis

In order to resist the statistical attacks, the encrypted images should possess certain random properties.

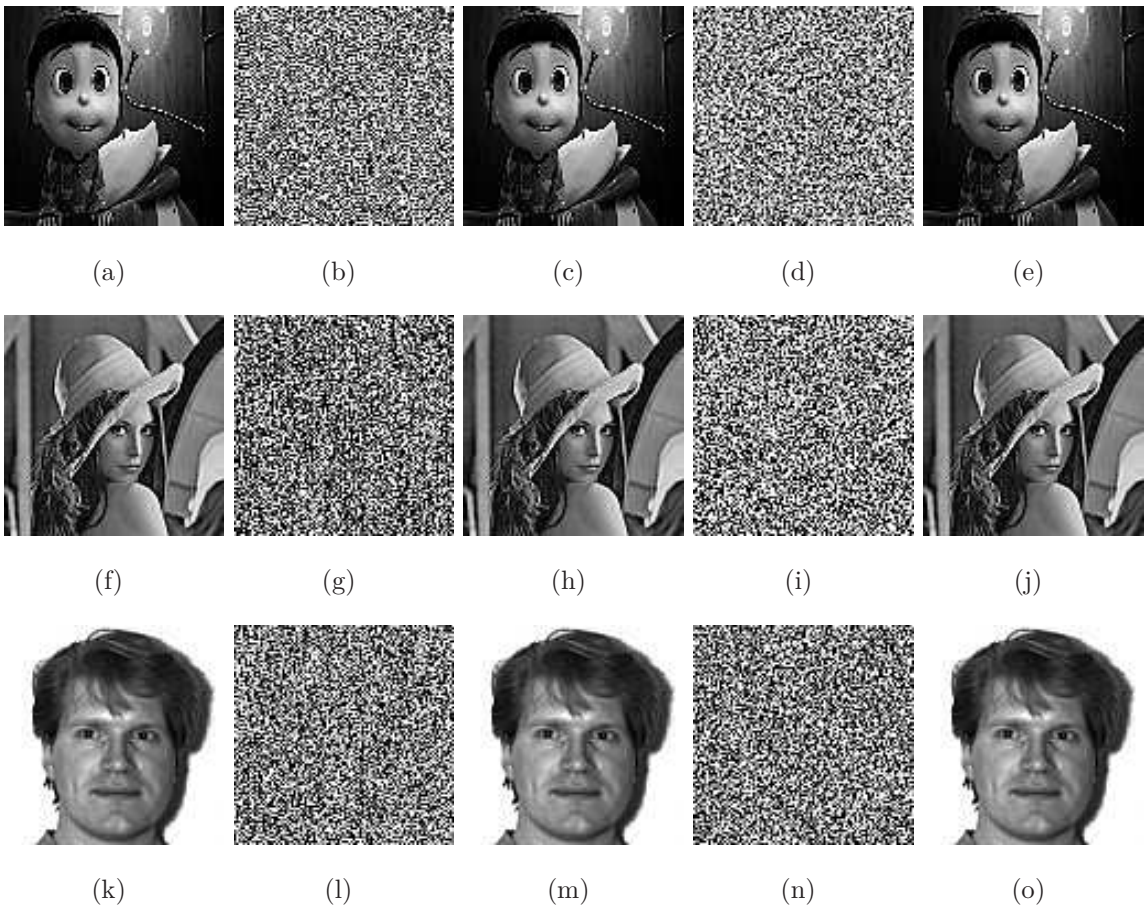


Figure 4.10: (a, f, k) Original 'Agnes', 'Lena' and 'Face' images, (b, g, l) corresponding encrypted images using chaos based DNA coding along with shifting and scrambling method, (c, h, m) corresponding decrypted images using chaos based DNA coding along with shifting and scrambling method, (d, i, n) corresponding encrypted images using chaos based DNA coding along with poker shuffling method, and (e, j, o) corresponding decrypted images using chaos based DNA coding along with poker shuffling method

Histogram of Encrypted Images

In order to appear random, the histograms of the encrypted images should be uniformly distributed in all gray levels. Figure 4.11 shows the histograms of original 'Agnes', 'Lena' and 'Face' images, corresponding encrypted and decrypted images by using both the proposed methods. From the histogram of the original images and corresponding histogram of encrypted images by using both the proposed methods, it is clear that the original pixel gray values are concentrated on some values, but the pixel gray values after the encryption are scattered in the entire pixel value space,

namely, two images have lower similarity. Clearly, it is difficult to use the statistical performance of the pixel gray value to recover the original image. Thereby, proposed algorithms has strong ability of resisting statistical attack. Figure 4.12(a, c, e) shows the scattered diagram between original and encrypted images using proposed chaos based DNA coding along with shifting and scrambling method. Figure 4.12(b, d, f) shows the scattered diagram between original and encrypted images using proposed chaos based DNA coding along with poker shuffling method. Figure 4.12 shows that, in both the proposed methods, the points are spread throughout the surface. That means weaker correlation occurs between original and encrypted images. Figure 4.13(a, c, e) shows the scattered diagram between original and decrypted images using proposed chaos based DNA coding along with shifting and scrambling method. Figure 4.13(b, d, f) shows the scattered diagram between original and decrypted images using proposed chaos based DNA coding along with poker shuffling method. Figure 4.13 shows that, in both the proposed methods, all the points are along a line. That means stronger correlation occurs between original and decrypted image.

Correlation of Adjacent Pixels

From the result of Table 4.2, it found that the correlation coefficient of the adjacent pixels in the encrypted image is very small, which is close to 0 for both the proposed methods and original image is almost close to 1. The average correlation coefficient is close to 0 for both the proposed methods. It clearly be seen that the proposed algorithms can destroy the relativity effectively; the proposed image encryption algorithms has a strong ability to resist statistical attack.

Table 4.2: Correlation coefficient of the adjacent pixels.

Correlation coefficient	Original images			Proposed encrypted images using chaos based DNA coding along with shifting and scrambling method			Proposed encrypted images using chaos based DNA coding along with poker shuffling method		
	Agnes	Lena	Face	Agnes	Lena	Face	Agnes	Lena	Face
Horizontal (H)	0.9120	0.8136	0.9730	-0.0291	-0.0075	-0.0003	-0.0014	-0.0137	0.0092
Vertical (V)	0.9335	0.9072	0.9803	-0.2136	-0.0096	-0.0304	-0.0147	-0.0038	0.0294
Diagonal (D)	0.8840	0.7734	0.9571	0.0134	0.0030	0.0149	-0.0086	-0.0092	-0.0096
$(H^2+V^2+D^2)^{0.5}$	1.5763	1.4433	1.6805	0.2160	0.0126	0.0338	0.0171	0.0169	0.0323
Average (H, V, D)	0.9098	0.8314	0.9702	-0.0764	-0.0047	-0.0053	-0.0083	-0.0089	0.0097

Figure 4.14, 4.15, and 4.16 shows the correlation distribution of two adjacent pixels for 'Agnes', 'Lena', and 'Face' images respectively by using both the proposed methods. From the contrast diagrams of Figure 4.14, 4.15, and 4.16 it can be observed

Table 4.3: Comparison of NPCR, UACI, MAE, and PSNR criteria of proposed methods

Criteria (expected value)		Original Image Vs. Encrypted Image	
		Proposed chaos based DNA coding along with shifting and scrambling method	Proposed chaos based DNA coding along with poker shuffling method
NPCR (99.61%)	Agnes	99.6900	99.7800
	Lena	99.5200	99.6300
	Face	99.4800	99.5800
UACI (33.46%)	Agnes	37.8034	39.8052
	Lena	29.3813	32.6649
	Face	35.9431	36.8410
MAE (Larger Value)	Agnes	96.3987	101.5033
	Lena	74.9223	83.2954
	Face	91.6549	93.9445
PSNR (Smaller Value)	Agnes	6.7937	6.4586
	Lena	8.8379	8.0827
	Face	7.1722	6.9582

that the correlation between pixels of original image is much larger than the correlation between pixels of encryption image, which means the adjacent pixels of original images have very strong linear correlation, while the correlation between adjacent pixels of encrypted images is very small. It has damaged the linear correlation of original image. Therefore both the proposed encrypted algorithms can effectively resist pixel correlation statistical attack.

4.7.2 Differential Analysis

To enumerate the difference between encrypted images and corresponding original images, three measures were adopted: Mean Absolute Error (MAE), the Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). Apart from that Peak Signal to Noise Ratio (PSNR) is also used to show the efficacy of the proposed methods.

The comparison of NPCR, UACI, MAE, and PSNR criteria of various images using the proposed chaos based DNA coding along with shifting and scrambling method and chaos based DNA coding along with poker shuffling method is shown in Table 4.3. The comparison of NPCR and UACI criteria of 'Lena' image using the proposed methods and the others is shown in Table 4.4. Table 4.5 shows the comparison of proposed methods with the other DNA papers.

The expected value of NPCR is found to be 99.61%. The proposed methods

are evaluated using this criterion and NPCR values of all the images using both the proposed methods are nearer equal to or greater than the expected value. The expected value of UACI can be computed as 33.46%, assuming each gray level is coded with 8 bits. The proposed method is evaluated using this criterion too and UACI values of all the images using both the proposed methods are also nearer equal to or greater than the expected value. The MAE values are larger for all the images by using both the methods. The PSNR values are smaller for all the images by using both the methods. Table 4.3 shows that the NPCR, UACI and MAE values are higher and on the other hand PSNR values are smaller for all the images by using proposed chaos based DNA coding along with poker shuffling. Table 4.4 reveals that the NPCR and UACI values of 'Lena' image by using the proposed methods are improved compared to the other reported methods.

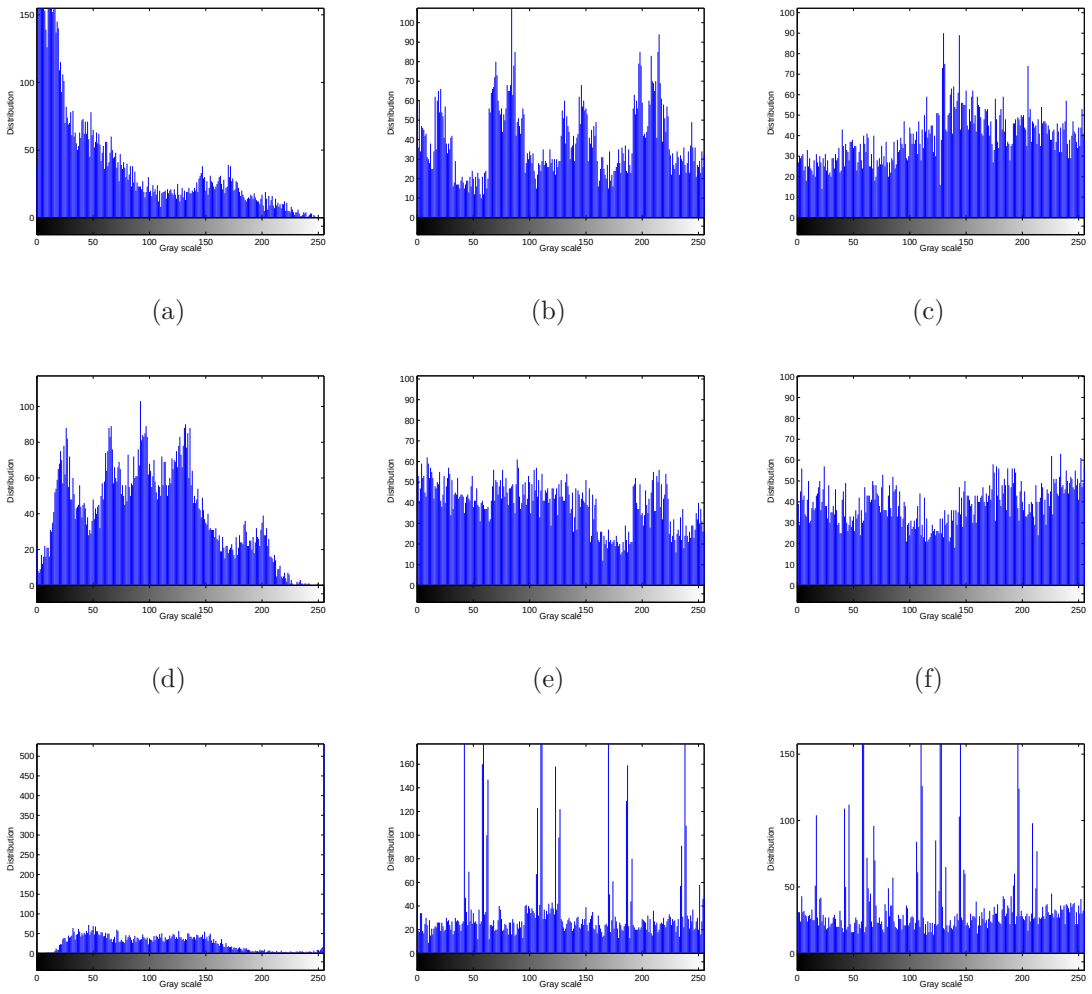


Figure 4.11: (a, d, g) Histogram of original 'Agnes', 'Lena', and 'Face' images, (b, e, h) Histogram of corresponding encrypted images using chaos based DNA coding along with shifting and scrambling methods, and (c, f, i) Histogram of corresponding encrypted images using chaos based DNA coding along with poker shuffling method

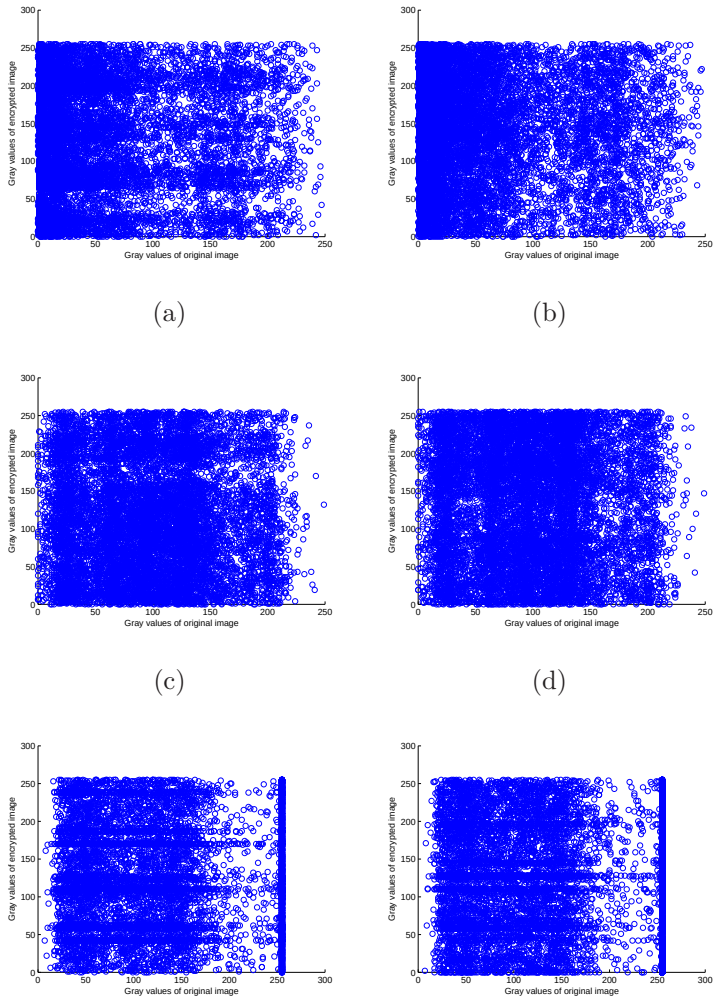


Figure 4.12: (a, c, e) Scattered diagram between original and encrypted images of 'Agnes', 'Lena' and 'Face' respectively using chaos based DNA coding along with shifting and scrambling method, (b, d, f) Scattered diagram between original and encrypted images of 'Agnes', 'Lena', and 'Face' respectively using chaos based DNA coding along with poker shuffling method.

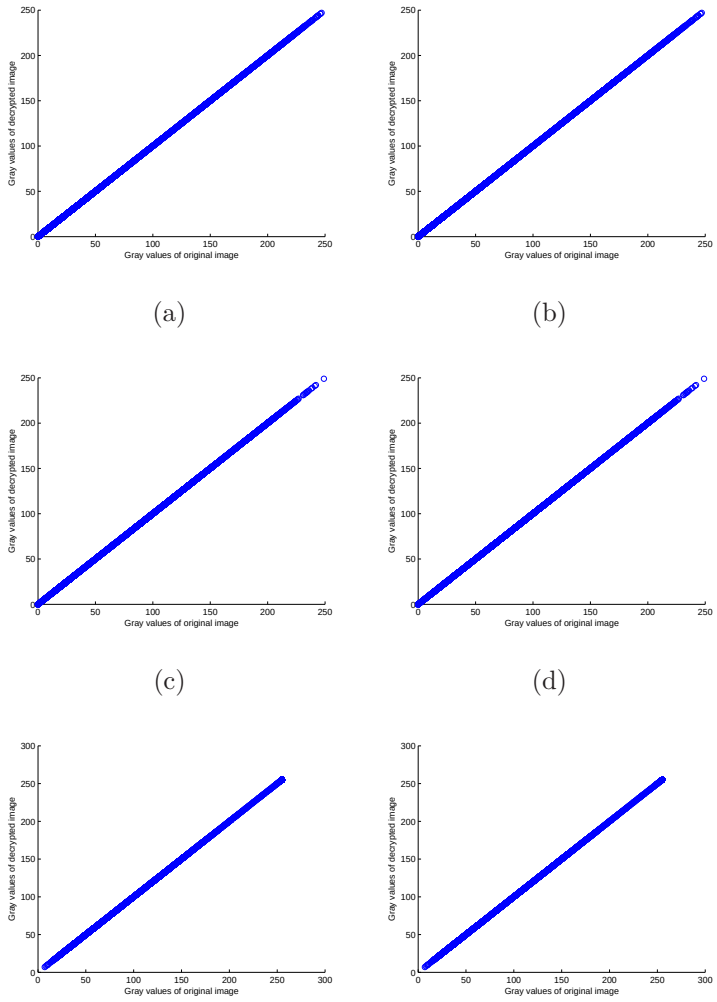


Figure 4.13: (a, c, e) Scattered diagram between original and decrypted images of 'Agnes', 'Lena', and 'Face' respectively using chaos based DNA coding along with shifting and scrambling method, (b, d, f) Scattered diagram between original and decrypted images of 'Agnes', 'Lena', and 'Face' respectively using chaos based DNA coding along with poker shuffling method.

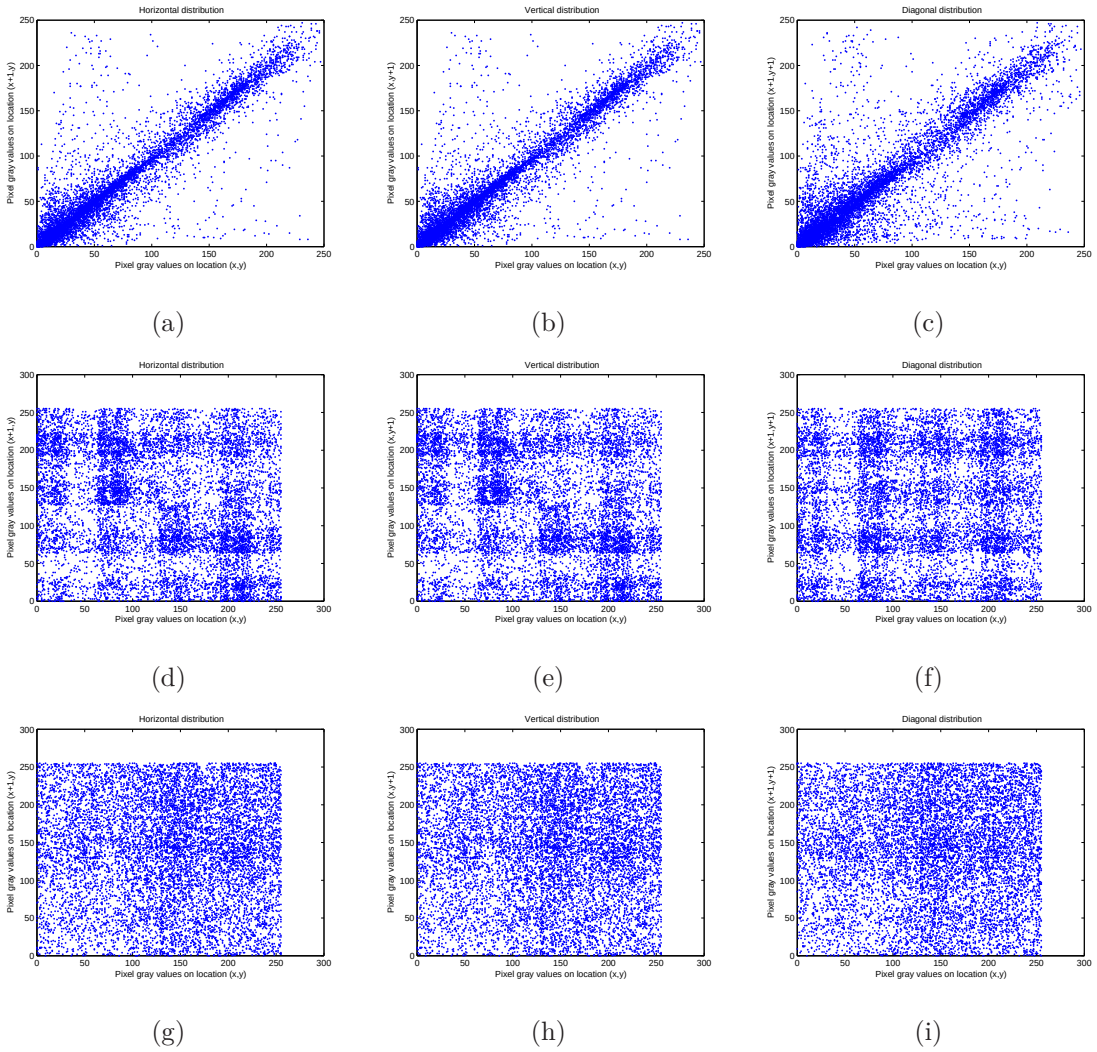


Figure 4.14: Correlation distribution of two adjacent pixels for 'Agnes' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed chaos based DNA coding along with shifting and scrambling method, and (g, h, i) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed chaos based DNA coding along with poker shuffling method

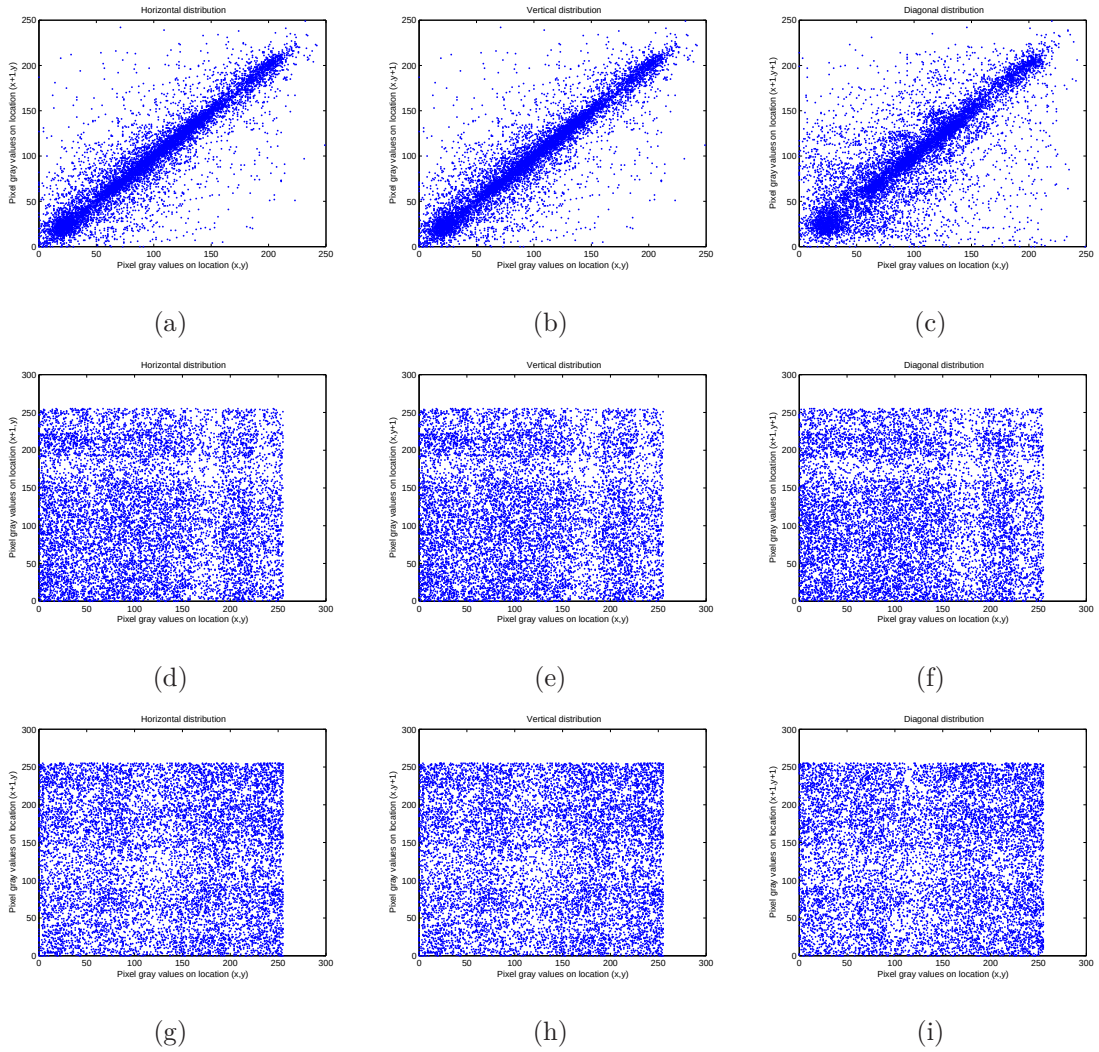


Figure 4.15: Correlation distribution of two adjacent pixels for 'Lena' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed chaos based DNA coding along with shifting and scrambling method, and (g, h, i) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed chaos based DNA coding along with poker shuffling method

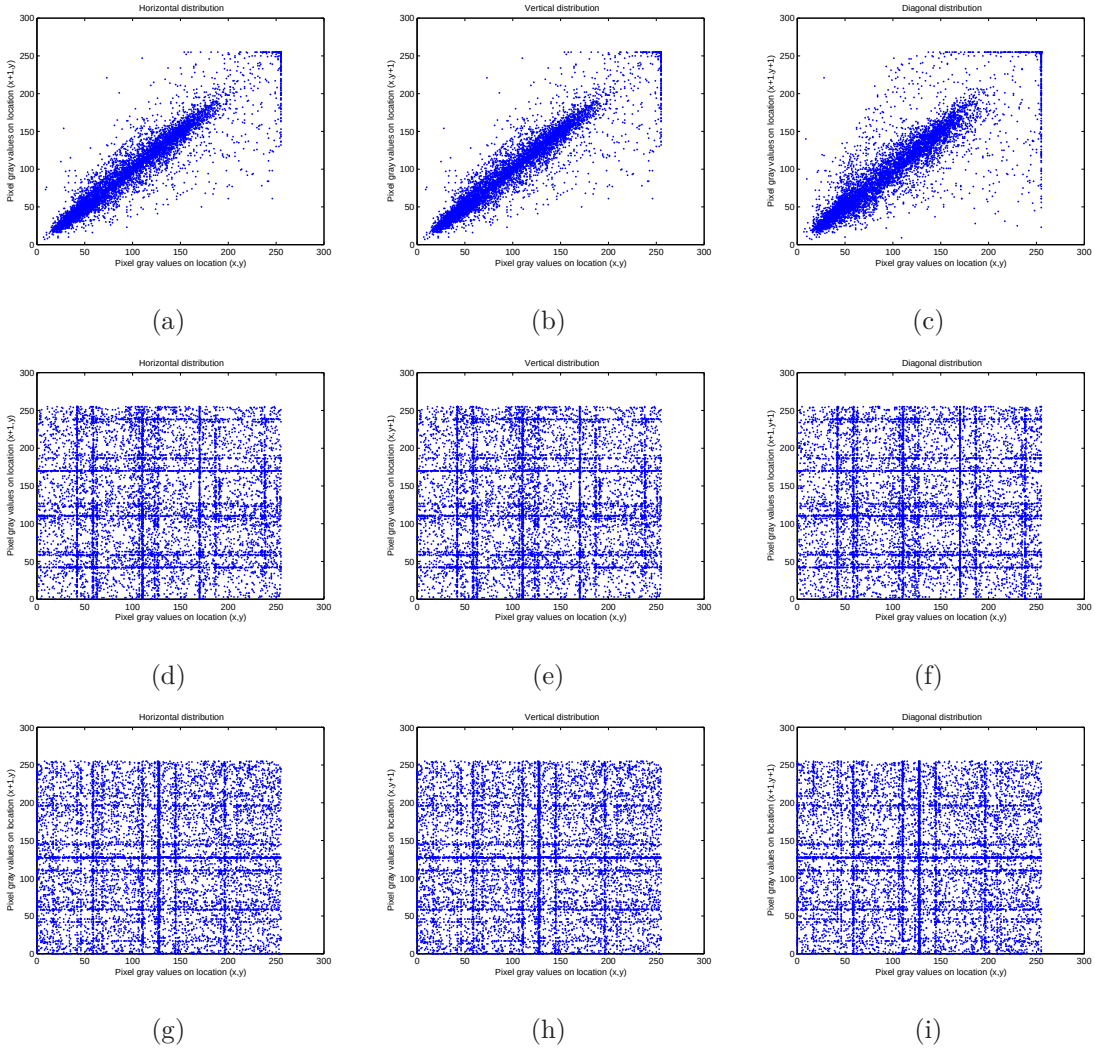


Figure 4.16: Correlation distribution of two adjacent pixels for 'Face' biometric image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed chaos based DNA coding along with shifting and scrambling method, and (g, h, i) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed chaos based DNA coding along with poker shuffling method.

Table 4.4: Comparison of NPCR, and UACI criteria of 'Lena' image by using both the proposed methods and the others

Criteria (expected value)	Original Image Vs. Encrypted Image					
	Zhang et al. [104] Second round	Zhou et al. [105] Second round	Mao et al. [106] First round	Borujeni et al. [98] First round	Chaos based DNA coding along with Shifting and Scrambling (Proposed Method-I)	Chaos based DNA coding along with poker Shuffling (Proposed Method-II)
NPCR (99.61)	21.5	25.0	37.0	99.7	99.6900	99.7800
UACI (33.46)	2.5	8.5	9.0	29.3	37.8034	39.8052

Table 4.5: Comparison of proposed methods with other DNA-based encryption algorithms

Considered items	Liu et al. [72]	Zhang et al. [70]	Gehani et al. [67]	Wang et al. [68]	Proposed Method-I	Proposed Method-II
Image	Yes	Yes	Yes	Yes	Yes	Yes
Text	No	Yes	Yes	No	No	No
Security Analysis	Yes	Yes	No	Yes	Yes	Yes
Biology Operation	Yes	No	Yes	Yes	Yes	Yes
Method	DNA complementary rule chaotic maps	DNA Subsequence operation chaotic maps	Use micro-array technology	Multilevel image encryption based on chaos and DNA coding	Chaos based DNA along with shifting and scrambling operation	Chaos based DNA along with poker shuffling operation

4.7.3 Measure of Entropy

The comparison of entropy between original images and encrypted images using the proposed chaos based DNA coding along with shifting and scrambling method, and proposed chaos based DNA coding along with poker shuffling method are presented in Table 4.6. A higher value of the entropy obtained in case of both the proposed methods indicates more randomness in the encrypted image resulting in better encryption. And also it shows that the proposed chaos based DNA coding along with poker shuffling method obtained more entropy value than the proposed chaos based DNA coding along with shifting and scrambling method.

Table 4.6: Entropy between original images and encrypted images of proposed methods

Images	Entropy		
	Original images	Encrypted images	
		Proposed chaos based DNA coding along with shifting and scrambling method	Proposed chaos based DNA coding along with poker shuffle method
Agnes	7.2437	7.8554	7.9338
Lena	7.5977	7.9377	7.9592
Face	5.9210	7.3421	7.4812

4.8 FPGA Implementation of Proposed Algorithm for Image Encryption

The invention of integrated circuits by Jack Kilby revolutionized the semiconductor world [107,108]. From that day, advancements in circuit design, manufacturing process and test are tremendous. Earlier versions of 8-bit, 16-bit and 32-bit microprocessors worked well in many applications. Due to miniaturization of transistors lead to number of transistors can be fabricated on single wafer became high. This has lead new generation of semiconductors known as System on Chips (SoC). Generally SoC's carry microprocessor, memory, system peripherals (PLL, voltage regulator, interrupt

controller) and application peripherals (ADC, CAN protocol controller, I2C, PWM module etc).

Parallel with above said advancements, various processor architectures are developed. These processors are developed to overcome the timing hazards and software implementation bottlenecks and to deliver high performance. The application verticals like consumer electronics, automobiles, communication systems, industrial and medical applications use signal processing, control engineering, cryptography and other system theories. Signal processing and control engineering requires more efficient processors to implement advanced algorithms.

Computational requirement of advanced algorithms is very high. Designing SoC's and processors to implement the complex advanced algorithms in real time is the requirement of the day. And also major semiconductor vendors are working towards to achieve in cost effective way. The research focus of our work is multilevel image encryption using chaos based DNA coding along with shifting and scrambling. The process described in Section 4.4 to perform the encryption is complex to implement in a FPGA without hardware software co-design. Implementation of image encryption using DNA encoding on advanced architectures like ARM processors can be done. For high performance applications, it is better to implement any complex mathematical technique in FPGA using hardware software co-design. Complete Field Programmable Gate Array (FPGA) hardware-software co-design solution can be achieved with the help of Electronic System Level (ESL) tools. ESL tools are also referred as system tools. The reputed system tools used to develop complex signal processing and control algorithm based applications are CoWare SPD (signal processing designer), MATLAB, and Celoxica Compiler and Synfora PICO tools. FPGA carry soft cores and hard cores along with programmable logic, such that these devices are best suitable for hardware-software co-design. Designers need to study algorithm holistically and to decide, which portion can be implemented as software and what will be hardware. With the results of simulation studies, it is easy to figure out computational bottlenecks. Through simulations, it is easy to figure out which part of computation takes much more time for execution. Time consuming portion can be implemented as custom hardware in programmable logic portion of FPGA and rest of the design can be implemented as software on soft-core processors (microblaze in the case of Xilinx FPGAs) or hard-cores (PPC or ARM) embedded inside the FPGA. Image encryption using DNA encoding is also a reasonably complex algorithm. The complexity lies in the creation of DNA matrix. Conversion of image

matrix into DNA (CATG) matrix is tedious task. And also, the creation of chaos matrix is also a similar type of problem. This is implemented in soft core processor microblaze on Xilinx FPGAs.

FPGA is an integrated circuit which can be programmable for any logic. Depending upon the size and programmable resources available on FPGA, user can program FPGA with a small digital circuit or a complex pipelined processor. The Xilinx FPGAs contain following cells: - (depending on the FPGA vendor, programmable cells and their components varies)

- Configurable Logic Blocks (CLB's) are evenly distributed across the FPGA. CLBs are comprises of slices. Slices comprise the look-up tables (LUTs) and multiplexers. Using LUTs and multiplexers and with combination of many slices any complex digital system can be realized.
- IOBs (input/output blocks) are located at the boundaries of the chip. Each I/O block contains different types of input output pins (ex: high speed to low speed, etc) used by designs during configuration.
- Clock buffer cells: clock buffer cells are delay cells, which are helpful in clock tree synthesis and timing adjustments.
- Multipliers.
- Dual port block RAMs.

CLB contains 4 slices and slice has two LUTs. They are connected together with the help of matrix of wires and programmable switches. The functionality of CLB is dependent on the values in the LUTs, which can be programmed. After the FPGA is being programmed with a bit stream, this essentially closes the switches in the interconnect matrix. This array of programmable logic and matrix of wires form the basis for complex FPGA designs. Apart from the above programmable logic portion, FPGAs also carries processor cores and other communication protocols like I2C, CAN etc. Knowledge of these soft and hard cores inside the FPGAs is also important for hardware software co-design. Xilinx FPGAs support soft processor microblaze. Microblaze is a 32-bit re-configurable soft core processor available from Xilinx. The architecture is shown in Figure 4.17. Microblaze is RISC core based on Harvard architecture proprietary of Xilinx. This processor is so flexible such that, for a given particular application particular features of processor and size of FPGA targeted.

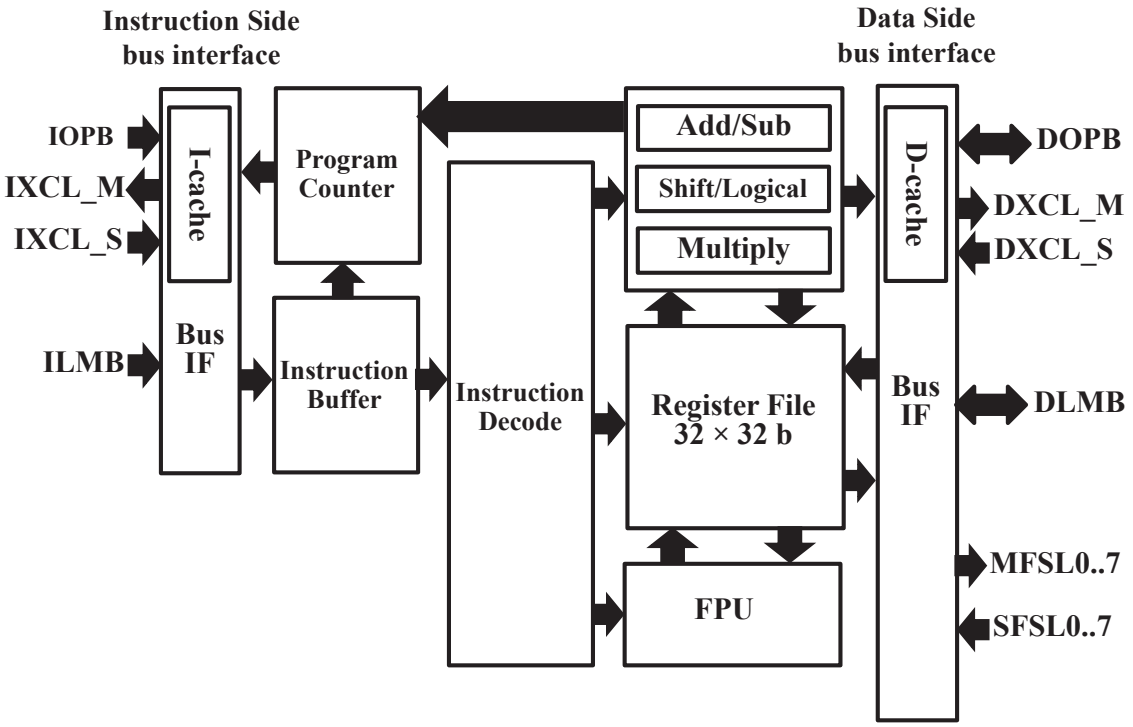


Figure 4.17: Architecture of microblaze processor

The user has the flexibility to enable required additional hardware in the core like integer multiplier, instruction cache, barrel shifter etc. The microblaze processor core can be connected with custom made application core located on the same chip in programmable logic area.

Most of the microcontrollers available today carry a processor (8 or 16 or 32-bit), memory and peripherals like interrupt controller, PLL, voltage regulator, ADC, PWM, I2C, CAN protocol etc. Co-processor (for ex: as in 8086 processor) and hardware accelerators are required to implement numerically complex algorithms like DNA coding based image encryption in an efficient way. The system on chip devices used in smart phones comprises of specialized IP cores for video processing, audio processing and wireless communication. This type of specialized hardware is required not only for signal processing applications, but also for control systems. A good example of such system is HCS12 microcontroller. HCS12 has got fuzzy logic coprocessor, using which fuzzy systems of reasonable size can be implemented in real time.

Microblaze processor will act like main processor and the custom co-processor or hardware accelerator can be designed in the available programmable logic space of FPGA. The hardware-software co-design of DNA coding based image encryption can

be implemented through this process in FPGA. In this work, hardware co-processor (for matrix addition, shifting, scrambling and complement) is tailored to handle the tasks which can be done in hardware in better way. The Figure 4.18 illustrates the concept.

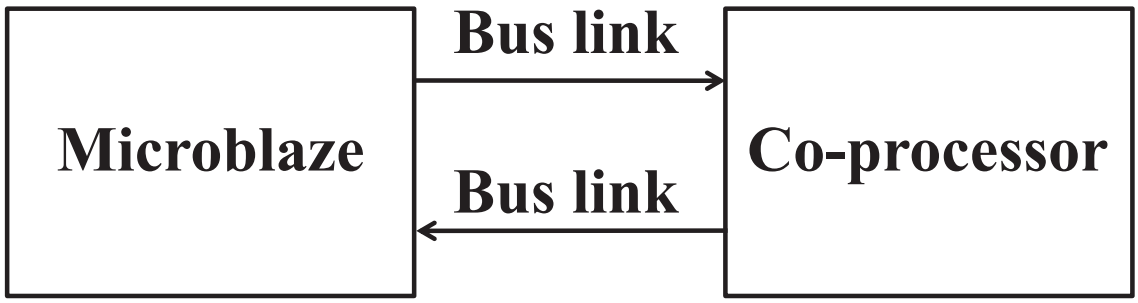


Figure 4.18: Communication between microbalze and co-processor

Xilinx ISE (Integrated Software Environment) is used Verilog programming to design coprocessor. Another platform tool from Xilinx called EDK is used to build interfacing between microblaze and co-processor. C programming is used to program the microblaze processor. Xilinx platform tool support programming of soft-core processor with good number of Application Programming Interfaces (API).

Microblaze and co-processor interface can be tightly coupled with the help of buses support by Xilinx and its tools. Availability of unidirectional links called Fast Simplex Links (FSL) on microblaze makes the interface with co processor tightly coupled. Microblaze supports eight FSL links. And also Xilinx provides instructions to program and establish the link between the microblaze and co-processor. Xilinx core generator is IP management utility. Xilinx provides few IP cores for designer's benefit. Core generator is useful in customizing the cores, which are available from Xilinx for an intended applications requirements.

4.8.1 FPGA Implementation

An Encryption system has the following components are: microblaze processor to perform DNA coding. The structure of hardware in programmable logic consists of matrix addition block, shifting and scrambling block. Microblaze microprocessor with embedded software controls and monitors the total system and provides an interface to co-processor. The embedded software running on microblaze performs DNA coding of the image, generating the chaotic sequence, DNA coding the chaotic

matrix. When DNA coded image and DNA coded chaotic matrix are ready, microblaze sends those matrices serially into matrix adder. Microblaze reads the output of adder and complements it accordingly. Again it sends complimented matrix back to co-processor to perform shifting and scrambling operation. Finally, microblaze reads back the matrix from the co-processor. Table 4.7 shows the number of slices used in Virtex-II Pro FPGA in implementation of image encryption based on chaos, DNA coding along with shifting and scrambling operation. Figure 4.19 depicts the verilog simulation result showing input and input. The simulation result showing intermediate signals has shown in Figure 4.20.

Table 4.7: Number of slices used in Virtex-II Pro FPGA

Sl. No.	DNA coding	No. of Slices used in Virtex-II Pro FPGA
1	Conventional Array Multiplier	815

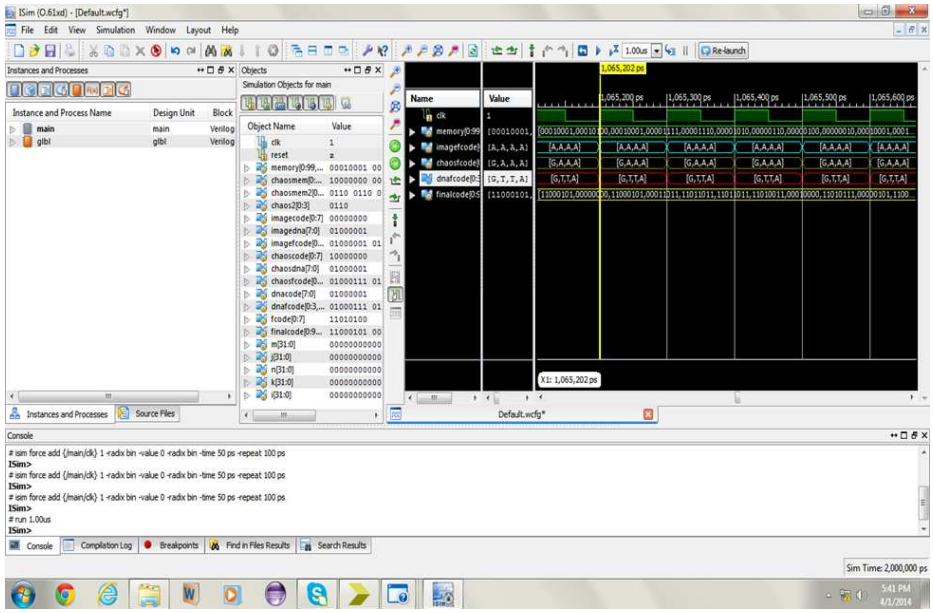


Figure 4.19: Verilog simulation result showing input and output

4.8.2 Conclusion of FPGA Implementation

Chaos based DNA coding along with shifting and scrambling image encryption is successfully implemented on FPGA using hardware-software co-design methodology. The complex algorithmic part of the scheme DNA coding of image matrix and generating chaotic sequence and corresponding DNA matrix is done in software

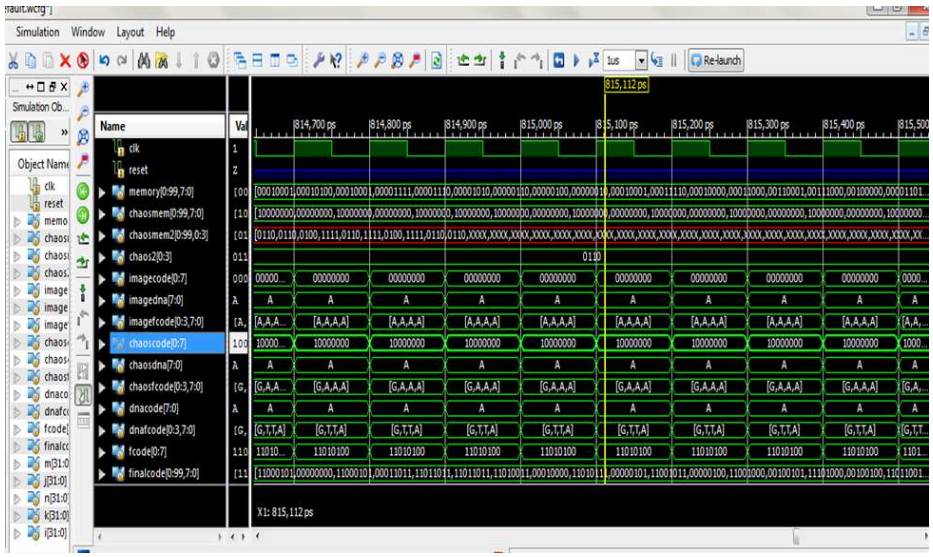


Figure 4.20: Verilog simulation result showing intermediate signals

running on microblaze processor. The other part matrix addition, shifting and scrambling can be done in an efficient way in hardware co-processor. The complete encryption scheme is successfully implemented and results are presented.

4.9 Summary

In this chapter, two distinct approaches for image encryption based on chaos based DNA coding along with shifting and scrambling or poker shuffle has been suggested. In the first approach, results obtained from chaos based DNA coding scheme is shifted and scrambled to provide encryption. On the other hand, in the second approach the results obtained from chaos based DNA coding encryption is applied to poker shuffle operation to generate the final result. Simulated results, security analysis and entropy suggest performance superiority for encryption and decryption of image and the results obtained have been compared with other competent methods. Following this FPGA implementation of proposed chaos based DNA coding along with shifting and scrambling cryptosystem has been performed.

Chapter 5

Development of a Secured Image Transaction and Authentication Scheme

Chapter 5

Development of a Secured Image Transaction and Authentication Scheme

Secured image transaction and authentication are important for many applications like e-commerce and military. The encryption methods proposed in chapters 2, 3 and 4 provides only confidentiality of information by encryption. Recent applications demand authenticity, integrity and non-repudiation of the information in addition to confidentiality. More over an ideal image cipher should be such that any adversary cannot modify the image and if any modifications are made, can be detected.

In this chapter a modified Hill cipher is proposed which is the combination of three techniques, those are suggested in [51] and [24] along with involutory key matrix generation method. This proposed modified Hill cipher takes advantage of all the three techniques. To achieve authenticity, integrity, and non-repudiation along with confidentiality, a novel hybrid method has been implemented. This method has employed proposed modified Hill cipher to provide confidentiality. Produced message digest encrypted by private key of RSA algorithm to achieve other features such as authenticity, integrity, and non-repudiation.

The rest of this chapter is organized as follows. In Section 5.1, the basic concept of message digest is presented. The basic concept of RSA algorithm is outlined in Section 5.2. In Section 5.3, modified Hill cipher for a large block of plaintext with interlacing and iteration is presented. Section 5.4 shows the proposed involutory key matrix generation method whereas Section 5.5, robust cryptosystem algorithm

is outlined. In Section 5.6 and 5.7 , proposed modified Hill cipher algorithm and proposed cryptosystem implementation is presented respectively. Finally, a summary of the chapter is presented in Section 5.8.

5.1 Message Digest

A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography" [109]. The input data is often called the message, and the hash value is often called the message digest or simply the digest.

Messages digest or hash function is used to turn input of arbitrary length into an output of fixed length, which is called the digest or hash of the input. This output can then be used in place of the original input. This has many advantages. The output always has the same length, so this can be taken into account when processing or storing the message digest. Also, the output is much shorter than the input, so that processing and storing can be done much quicker.

To make hash functions work, they should have two properties:

a. **Reverting a digest function to recover the input:** The first property prevents people from taking a particular digest and using it in connection with another message. The digest should be published in a newspaper, which proves that one had access to the input message on that date. No one else can know the message, because of this first property.

b. **Finding two inputs with the same digest:** The second property means that if two inputs produce the same message digest, they must be the same input as well. Often the second requirement is taken even further: if a message is changed slightly, the message digest of the changed message would have large change.

Figure 5.1 shows the technique for secured message transaction using message digest concatenation [77]. This technique involves the use of hash function to generate a small fixed-size block of data, known as cryptographic check-sum or message digest (MD) that is appended to the message. This technique assumes that the two communicating parties say 'A' and 'B', share the same process of digest generation.

When 'A' has a message to send it to the destination 'B', first it generates the message digest (MD) of the message and then concatenate it with that message, after that the message plus the MD are transmitted to the destination 'B'. Then 'B' performs the same operations as the message digest generation function of 'A' to produce the MD. If only the receiver and the sender know the process of message digest generation technique and if the received MD and the generated MD matches, then:

i. the receiver B is assured, that the message has not been altered. If an attacker alters the message but does not alter the digest MD, then the receiver's generation of MD will differ from the received MD.

ii. the receiver is assured that the message is from the alleged sender. Because, no one else knows the message digest generation techniques, no one else could prepare a message with proper MD.

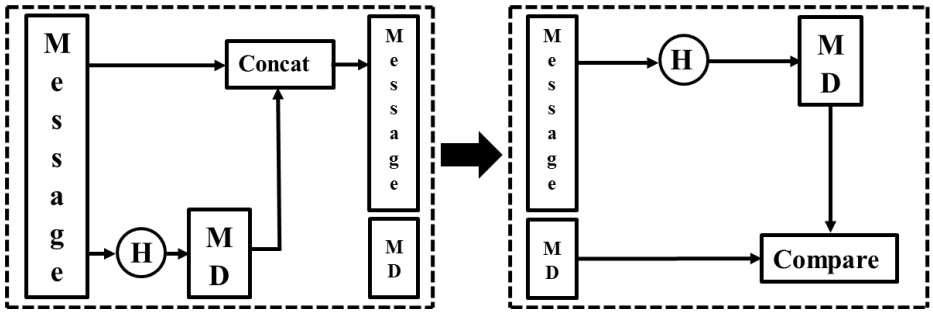


Figure 5.1: Secured message transaction using message digest concatenation

5.1.1 Cross Concatenation of Message Digest

Figure 5.2 shows the secured message transaction using message digest cross-concatenation. This system has an added feature of extra security by splitting the message into two halves and cross concatenating MD inside the Message. The encrypted mixed two halves contains half of the message and half of the MD inter weaved inside one another making an interceptor almost impossible to accurately guess the original message.

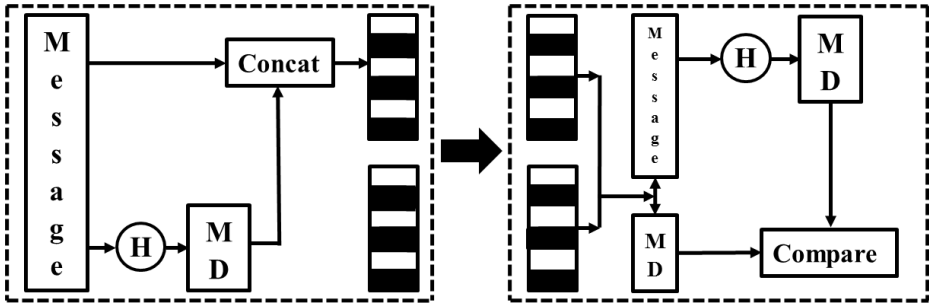


Figure 5.2: Secured message transaction using message digest cross-concatenation

5.1.2 Applications of Message Digest/Cryptographic Hash Functions

i. Digital signatures: A popular application of message digests or hash functions is digital signatures. Computing a digital signature for a long message is very time-consuming. However, computing a digital signature for a message that is only 128 or 160 bits long can be done quickly. So, instead of digitally signing the message, the message's hash is signed. To verify the signature, the recipient of the message computes the hash of the message received. He compares this against the fingerprint that was signed. If they are the same, then (because of the second property above), the message he received is authentic. Should an attacker have manipulated the message, then the fingerprint of the manipulated message will be very different from the fingerprint that has been signed by the sender. The attacker is not able to create a new fingerprint that is signed by the original sender.

ii. Integrity verification: File transmissions over networks such as the Internet may sometimes introduce small errors. To verify whether the received file is identical to the original, the recipient computes the hash of the received file. This hash is then compared to the hash of the original file. That original hash was published on the website or FTP site where the original can be downloaded. It could also be transmitted along with the file. This use of hash functions is comparable to the use of checksums or Cyclic Redundancy Check (CRC) functions. However CRC functions typically produce outputs of only 32 bits long. It is easy to find a different input that produces the same 32-bit output. In this scenario, tampering with the original file cannot be detected. If that is also desirable, the creator of the original file should not just publish the hash but should digitally

sign that hash first.

iii. Message authentication codes: A Message Authentication Code (MAC) is somewhat similar to a digital signature. Sometimes a MAC is called a keyed hash function. The sender creates the MAC using the message to be authenticated and a secret key. The recipient verifies that the MAC is authentic using this same secret key. This is different from digital signatures, where a public/private key pair is used.

5.2 RSA Algorithm

The details of RSA algorithm that means key generation algorithm, encryption algorithm, decryption algorithm as well as their applications are described in Section 3.4 of Chapter 3.

5.3 Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration

Sastry et al. [51] have proposed an algorithm that employs interlacing in the process of encryption and decomposition in the process of decryption. Use of iterations in encryption makes the process complex and secure. Interlacing means the interchange of binary bits of message matrix element. Iteration means to execute this interlacing process in definite loop. Here, it is to be noted that decomposition is a reverse process to that of interlacing.

5.3.1 Algorithm for Interlacing and Decomposition

1. Convert all elements of matrix into 8 bit binary form.

2. New dimension is $n \times n \times 8$. Divide this new matrix into two matrixes with dimension $n \times n \times 4$.

3. Interchange $(2m)^{th}$ column of first matrix with $(2m-1)^{th}$ column of second matrix with m varies from 1 to $2n$.

4. Combine two matrixes to create new $n \times n \times 8$ matrix.

5. Convert 8 bit elements into decimal numbers and to get $n \times n$ matrix.

6. This matrix is interlaced and different from the original matrix.

Advantage of modified Hill cipher technique is that it is secure from known plaintext attack. By the knowledge of plaintext, key cannot be determined as encryption takes place many number of times in the iteration loop. Cryptanalysis and avalanche effect have proved the above advantage. Sastry et al. [51] have proposed modified Hill cipher technique for a data block. While using this for encrypt image following problem arise and those are:

- If the image matrix, key matrix or inverse of key matrix contains elements with decimal values then the elements cannot be changed into binary form and process will not be correct.
- The key matrix used must have to be invertible, so that decryption can take place.

Hence solution to above problems has been proposed and used for the image encryption. The modification includes

- All the elements should be pure integer so that they can be changed into binary form.
- An involutory matrix with integer elements is used for encryption and decryption.

5.4 Involutory Key Matrix Generation Method

As discussed in previous chapter Hill cipher requires inverse of the key matrix while decryption. The fact that not all the matrices have an inverse and hence will not be eligible as key matrices in the Hill cipher scheme. Modified Hill cipher using interlacing and iteration cannot be used for encrypting an image because of the loss of data during interlacing (binary conversion and rearrangement) of temporary cipher though it provides a robust encryption. So use of involutory key matrix eliminates the possibility of any decimal value and makes the modified Hill cipher evenly applicable to images too. Algorithm for involutory key matrix generation was proposed and presented in Section 2.3 of Chapter 2 .

5.5 Robust Cryptosystem Algorithm

Rushdi et al. [24] in their research paper "Design of a robust cryptosystem algorithm for non-invertible matrices based on Hill cipher," have proposed an efficient technique for safe transmission of cipher and key. This technique can also be used with Hill cipher algorithm to overcome its major problem of non-invertible key matrix. This new method depends on the idea that on the encryption side, each plaintext character is converted into two ciphertext characters, and on the decryption side each set of two ciphertext characters are converted into one plaintext character. In this way we can use any key matrix (invertible or not) and also, the key generation that was always difficult when the key was non-invertible has been solved.

5.5.1 Algorithm for Encryption

1. Convert the plaintext characters into numerical numbers.
2. Check if the determinant matrix is zero then add identity matrix else no operation required.
3. Calculate the column vector,
$$c = k \times x \tag{5.1}$$
4. Calculate
$$c_1 = fix\left(\frac{c}{p}\right) \ and \ c_2 = mod(c, p) \tag{5.2}$$
5. Convert the numerical numbers (c_1, c_2) into characters.

5.5.2 Algorithm for Decryption

1. Convert the two sequence of ciphertext into numerical numbers (y_1, y_2).
2. Check if the determinant matrix is zero then add identity matrix else no operation required.
3. Calculate the column vector
$$p = inv\,(k) \times ((y_1 * 26) + y_2) \tag{5.3}$$
4. Convert the numerical numbers p into characters.

5.6 Proposed Modified Hill Cipher Algorithm

To prevent adversary attack and to ensure a healthy recognition system, the biometric templates are encrypted before transmission or storing in database. Different cryptographical techniques are used for encrypting and decrypting the templates depending upon the level of optimization between security and speed of response of the biometric system. Proposed modified Hill cipher algorithm can be employed to encrypt biometric templates.

This section presents the proposed technique for encryption and decryption of image efficiently. This cryptographic system is a combination of the modified Hill cipher for large block of plaintext with interlacing and iteration [51] along with involutory key matrix generation method and robust cryptosystem [24]. The combined cryptosystem takes advantage of all the three techniques. The encryption and decryption algorithms are presented:

5.6.1 Algorithm for Encryption

1. The template image is converted to a square matrix P.
2. A non-singular involutory key matrix K is considered with same order as the size of the template image.
3. The image matrix P is encrypted by using modified Hill cipher technique with involutory key based on binary interlacing and iteration as explained in Section 5.3.
4. The cipher C created above is split into two parts C_1 and C_2 as explained in Section 5.5.

5.6.2 Algorithm for Decryption

1. The two parts of cipher are joined together to form the encrypted image matrix C as
$$C = (C_1 * x) + C_2 \tag{5.4}$$
2. The ciphertext so formed is decrypted using modified Hill cipher using interlacing and iteration as explained in Section 5.3.
3. The recovered matrix P is the decrypted image or template.

The encryption and decryption process is illustrated by flow diagram in Figure 5.3. $Interlace, decompose, fix$ and mod are the functions for performing modified Hill cipher and robust cryptosystem algorithm.

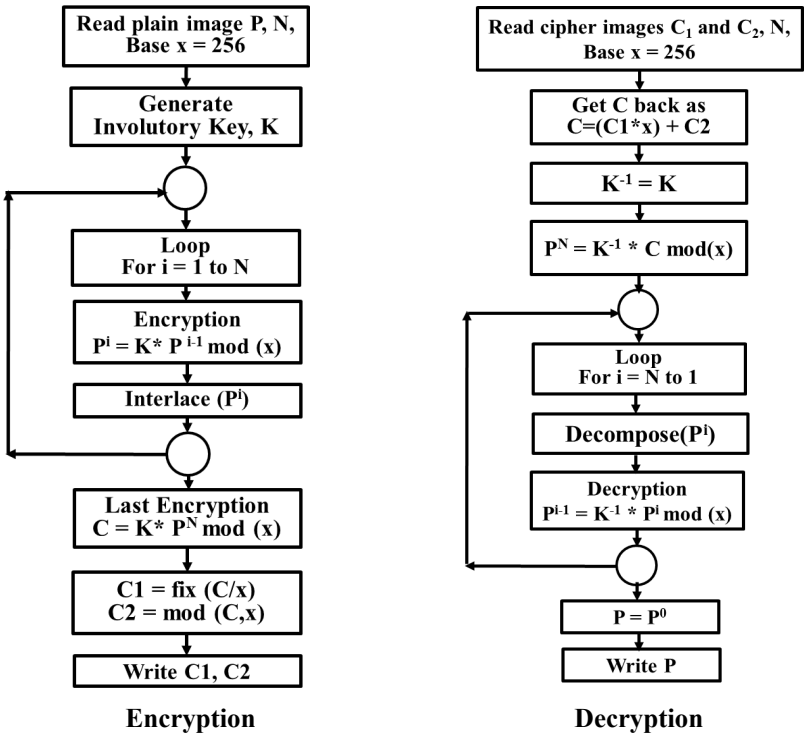
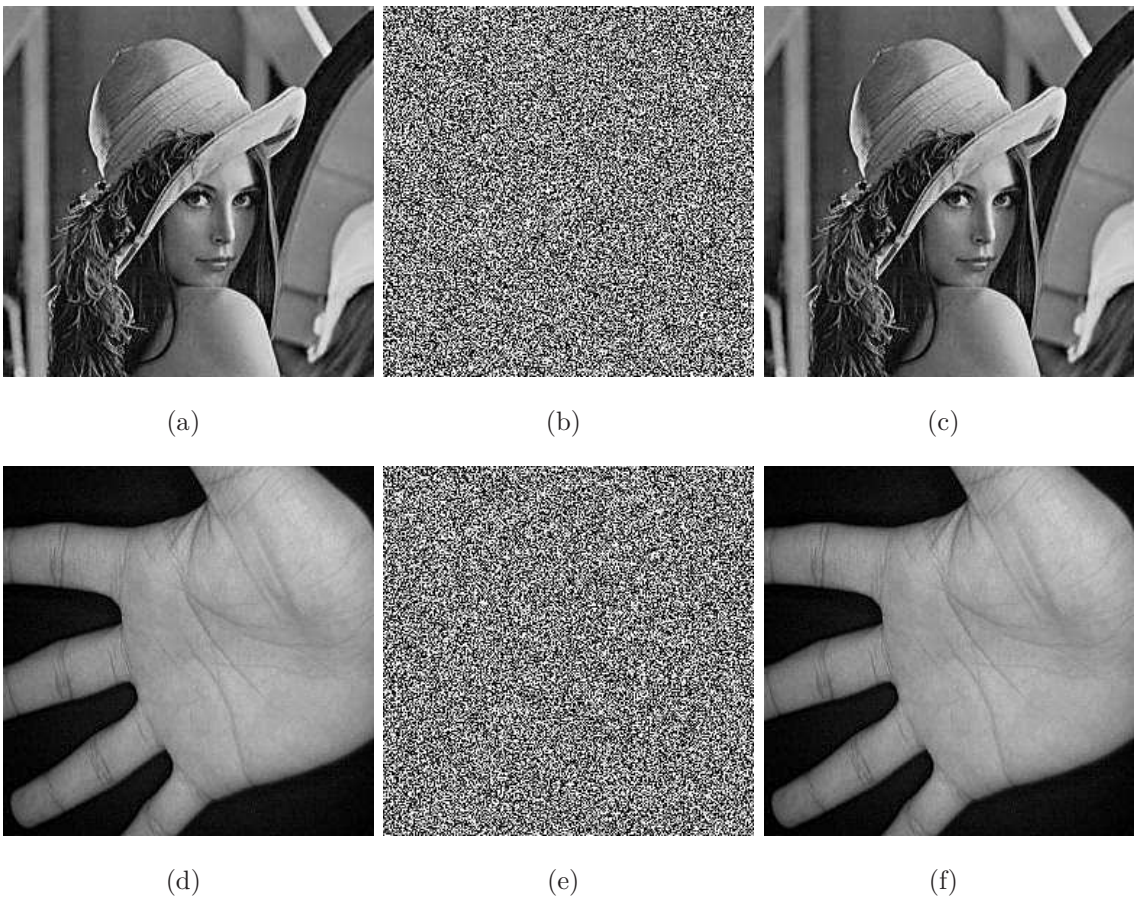


Figure 5.3: Flow diagram of proposed modified Hill cipher technique for encryption and decryption

5.6.3 Simulation Results

Different images are encrypted and decrypted using proposed modified Hill cipher algorithm and the results are shown in Figure 5.4 (C_1 and C_2 are joined together to get the encrypted image output). In Figure 5.4(b, e), it is cleared that proposed modified Hill cipher algorithm can able to encrypt the images properly. In Figure 5.4(c, f), it shows that there is no loss of data during decryption. So the proposed modified Hill cipher method is applicable to protect both conventional and biometric images during communication and transmission. The palmprint biometric image is taken from the CASIA (Chinese Academy of Sciences' Institute of Automation) image database [99].



(a) (b) (c)

(d) (e) (f)

Figure 5.4: (a, d) Original 'Lena', 'Palmprint' images, (b, e) corresponding encrypted images, and (c, f) corresponding decrypted images

5.6.4 Security Analysis and Discussion

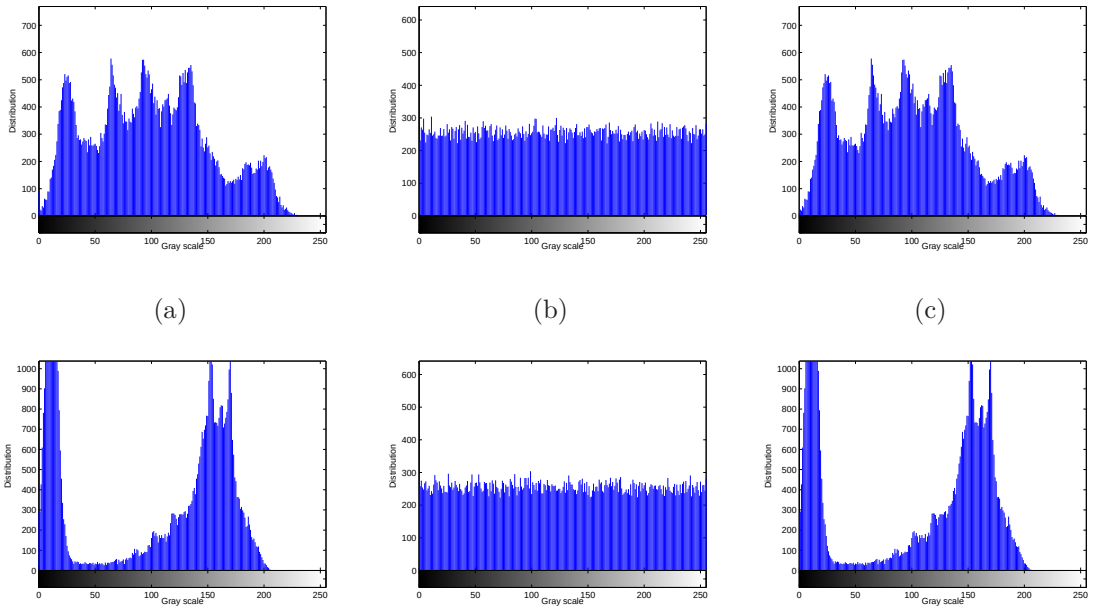
Some security analysis has been performed on the proposed encryption technique which includes statistical analysis (histogram, scattered diagram, correlation coefficient), differential analysis, and entropy measure. The security analyses for the proposed modified Hill cipher algorithm are discussed as follows.

Statistical Analysis

Histogram of Encrypted Image:

To resist statistical attack, the histograms of the encrypted images should be uniformly distributed in all gray levels. A detail study has been conducted and the results are summarized as followings. Different images have been tested, and similar results are obtained. Figure 5.5 shows the histograms of original and corresponding encrypted

images using proposed modified Hill cipher algorithm. It compares the gray histogram of the images before and after encryption to analyze the statistical performance. From Figure 5.5, it shows that the original pixel gray values are concentrated on some value, but the pixel gray values after the encryption are scattering in the entire pixel value space, namely, two images have lower similarity as a result gives high quality of encryption. Thereby, the proposed algorithm has strong ability of resisting statistical attack. Also there is no loss of data in decryption. So the proposed method is applicable to protect both conventional and biometric images during communication and transmission. Figure 5.6(a, c) shows the scattered diagram between original and encrypted images using the proposed modified Hill cipher algorithm. It shows that, all the points spread throughout the surface. That means weaker correlation occurs between original and encrypted images. Figure 5.6(b, d) shows the scattered diagram between original and decrypted images using proposed modified Hill cipher algorithm. It shows that, all the points are along a line. That means stronger correlation occurs between original and decrypted images.



(a) (b) (c)

(d) (e) (f)

Figure 5.5: (a, d) Histograms of original 'Lena' and 'Palmprint' images respectively, (b, e) Histograms of corresponding encrypted images by using proposed modified Hill cipher algorithm, (c, f) Histograms of corresponding decrypted images by using proposed modified Hill cipher algorithm respectively.

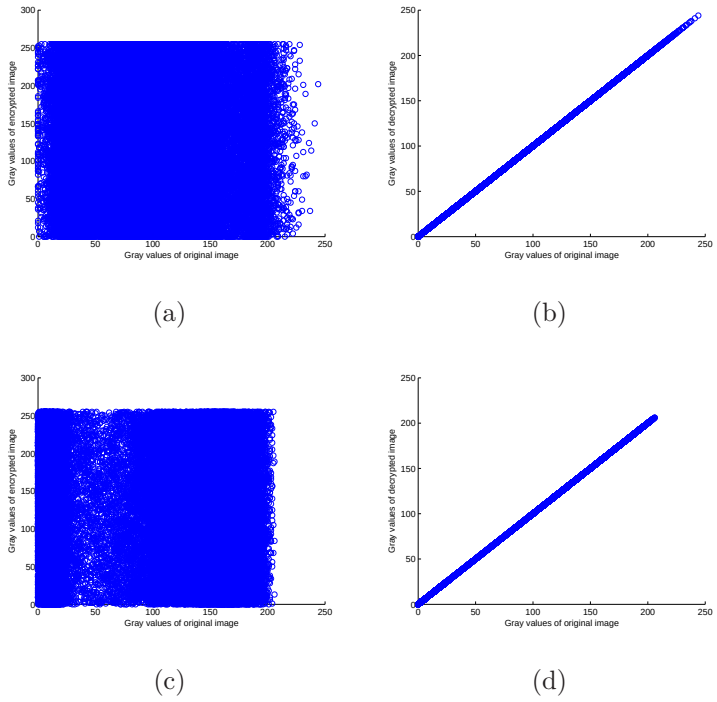


Figure 5.6: (a, c) Scattered diagram between original and encrypted images of 'Lena' and 'Palmprint' respectively by using proposed modified Hill cipher algorithm, (b, d) Scattered diagram between original and decrypted images of 'Lena' and 'Palmprint' respectively by using proposed modified Hill cipher algorithm.

Correlation of Adjacent Pixels:

From Table 5.1, it found that the correlation coefficient of the adjacent pixels in the encrypted image is very small, which is close to 0 for the proposed modified Hill cipher algorithm and original image is almost close to 1. The average correlation coefficient is close to 0 for the proposed modified Hill cipher algorithm. It clearly be seen that the proposed algorithm can destroy the relativity effectively; the proposed image encryption algorithms has a strong ability to resist statistical attack.

Figure 5.7 and 5.8 shows the correlation distribution of two adjacent pixels for 'Lena' and 'Palmprint' images respectively by using the proposed modified Hill cipher algorithm. From the contrast diagrams of Figure 5.7 and 5.8 it observed that the correlation between pixels of original images is much larger than the correlation between pixels of encrypted images. That means, the adjacent pixels of original images has very strong linear correlation, while the correlation between adjacent pixels of encrypted images is very small. It has damaged the linear correlation of original image. Therefore the proposed encrypted algorithm can effectively resist

pixel correlation statistical attack.

Table 5.1: Correlation coefficient of adjacent pixels of original images and their corresponding encrypted images by using proposed modified Hill cipher technique.

Correlation coefficient	original images		Encrypted images using modified Hill cipher algorithm	
	Lena	Palmprint	Lena	Palmprint
Horizontal (H)	0.9384	0.9971	-0.0038	-0.0071
Vertical (V)	0.9698	0.9963	-0.0058	-0.0103
Diagonal (D)	0.9164	0.9929	0.0082	-0.0040
$(H^2 + V^2 + D^2)^{0.5}$	1.6312	1.7242	0.0107	0.0132
Average (H, V, D)	0.9415	0.9954	-0.0005	-0.0072

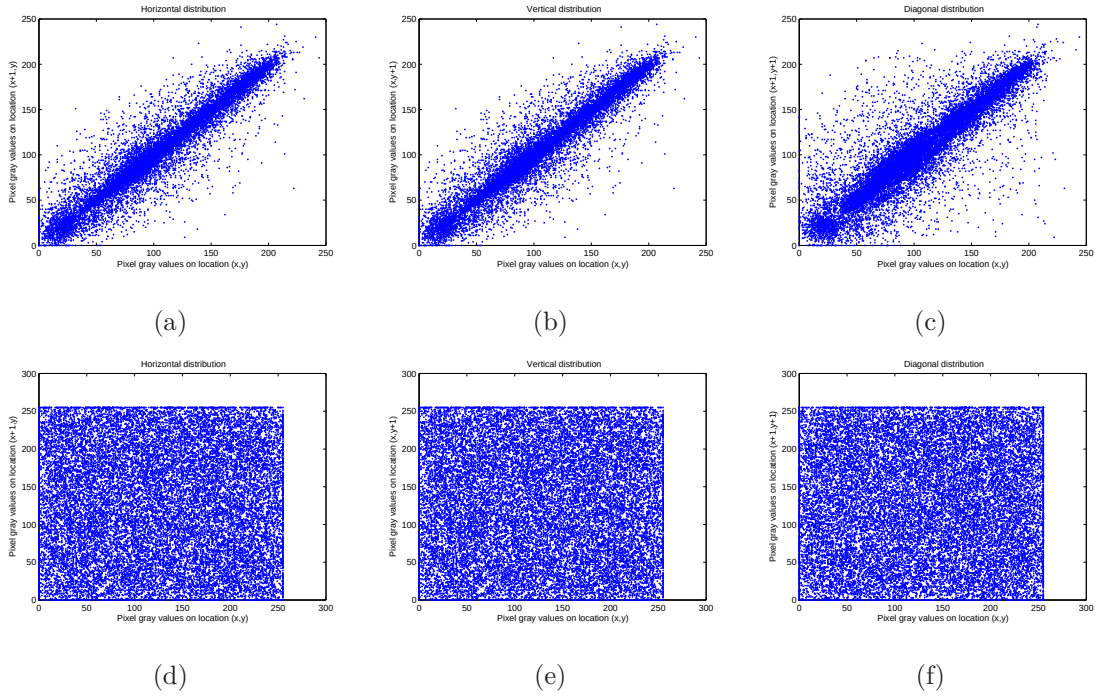


Figure 5.7: Correlation distribution of two adjacent pixels for 'Lena' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using modified Hill cipher algorithm.

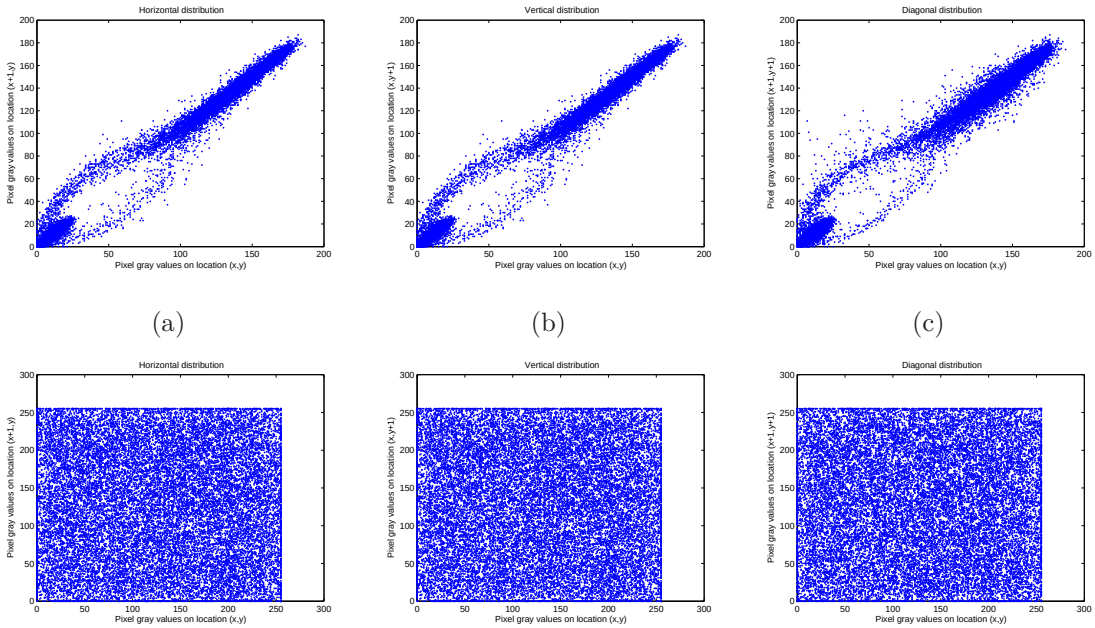


Figure 5.8: Correlation distribution of two adjacent pixels for 'Palmprint' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using modified Hill cipher technique.

Differential Analysis

The major requirement of all the encryption techniques is the encrypted image should be significantly different to the original one. To quantify the difference between original image and corresponding encrypted image, three measures were used: Mean Absolute Error (MAE), the Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). Apart from that, Peak Signal to Noise Ratio (PSNR) is also used to show the efficacy of the method.

The comparison of NPCR, UACI, MAE, and PSNR criteria of 'Lena' and 'Palmprint' images using the proposed modified Hill cipher algorithm is shown in Table 5.2. The comparison of NPCR, UACI, MAE, and PSNR criteria of the same images in various iterations using the proposed modified Hill cipher algorithm is shown in Table 5.3.

From Table 5.2, it found that, the NPCR value of 'Lena' image is equal to the expected NPCR value and 'Palmprint' image is 0.022% higher than the expected

Table 5.2: Comparison of NPCR, UACI, MAE, and PSNR criteria of 'Lena' and 'Palmprint' images by using proposed modified Hill cipher algorithm

Criteria (expected value)		Original Image Vs. Encrypted Image
NPCR (99.61%)	Lena	99.6109
	Palmprint	99.6323
UACI (33.46%)	Lena	30.6395
	Palmprint	32.7206
MAE (Larger value)	Lena	78.1307
	Palmprint	83.4377
PSNR (Smaller value)	Lena	8.5859
	Palmprint	7.9692

NPCR value. Similarly, the UACI value of 'Lena' image and 'Palmprint' image is nearer equal to the expected UACI value. The MAE values are larger for all the images. Consequently the PSNR values are smaller for all the images.

In this proposed method, each plain image is converted into two cipher images and on the decryption side each set of two cipher images is converted into one plain image. Flaws of original Hill cipher algorithm like known plaintext attack and key inversion problem solved in the proposed modified Hill cipher algorithm. For analysis after encryption both the cipher are combined and formed a single encrypted image. As a result, the proposed algorithm has a strong ability to encrypt an image against any attack. From Table 5.3, it is observed that the NPCR, UACI and MAE values are gradually increases by increasing the number of iterations. Similarly the PSNR values are gradually decreases by increasing the number of iterations.

5.6.5 Measure of Entropy

The comparison of the entropy between original images and encrypted images using the proposed modified Hill cipher algorithm is presented in Table 5.4. A higher value of the entropy obtained in case of proposed algorithm indicates more randomness in the encrypted image resulting in better encryption.

Table 5.3: Comparison of NPCR, UACI, MAE, and PSNR criteria of 'Lena' and 'Palmprint' images by using proposed modified Hill cipher algorithm in various iterations

Criteria		I-1	I-2	I-4	I-8	I-12	I-16
NPCR	Lena	94.1589	98.8770	99.3958	99.5880	99.5956	99.6109
	Palmprint	98.9349	99.5972	99.6033	99.6140	99.6216	99.6323
UACI	Lena	22.2619	30.5520	30.5112	30.5469	30.6127	30.6395
	Palmprint	28.5458	32.1307	32.7013	32.7198	32.7204	32.7206
MAE	Lena	56.7678	77.9076	77.8035	77.8945	78.0624	78.1307
	Palmprint	72.7918	83.1086	83.2469	83.4076	83.4371	83.4377
PSNR	Lena	10.7907	8.9032	8.8986	8.8234	8.5889	8.5859
	Palmprint	9.1572	7.9875	7.9837	7.9812	7.9698	7.9692

Table 5.4: Entropy between original images and encrypted images using proposed modified Hill cipher algorithm

Images	Entropy	
	Original images	Encrypted images by using the proposed modified Hill cipher algorithm
Lena	7.5977	7.9564
Palmprint	6.9319	7.9575

5.7 Algorithm for Cryptosystem Using Modified Hill Cipher

The proposed modified Hill cipher algorithm is employed to construct a cryptosystem which not only ensures the privacy but also provides authenticity, integrity and non-repudiation. It also provides two level securities to the image. This cryptosystem comprises of proposed modified Hill cipher algorithm, RSA and bit-XOR method. Image to be transmitted is encrypted by using proposed modified Hill cipher algorithm. Message digest of the image is generated by using bit-XOR method. This message digest is then encrypted by private key of RSA algorithm and this acts as digital signature. Encrypted message digest is cross-concatenated with encrypted image and

transmitted to receiver end.

On the receiver side, the cross-concatenated encrypted message digest and encrypted image received in two parts are separated as, encrypted image and encrypted message digest. In one part encrypted image is decrypted by using modified Hill cipher and in other part encrypted message digest is decrypted by using RSA public key. After decryption, in one part original image is recovered and in other part message digest is recovered. From the recovered image message digest is generated by using bit-XOR method. Finally, the recovered message digest and generated message digest is checked for authenticity.

5.7.1 Encryption Algorithm

1. Image converted into 256×256 matrixes.
2. Involutory key matrix is generated by using proposed involutory key matrix generation method presented in Section 2.3 of Chapter 2.
3. Generate the message digest from the image by performing 3-times bit-wise XOR operation of the image.
4. Encrypt image by using proposed modified Hill cipher technique presented in Section 5.6.
5. Encrypt the message digest by using RSA private key presented in Section 3.4 of Chapter 3.
6. Finally, encrypted message digest with the encrypted image is cross-concatenated. The cross-concatenated encrypted message digest along with image is transmitted in two parts to the receiver side.

5.7.2 Decryption Algorithm

1. At the receiver side, cross-concatenated encrypted message digest along with encrypted image received in two parts are separated back, forming of two parts as encrypted image and encrypted message digest.
2. Then the encrypted image is decrypted by using proposed modified Hill cipher technique presented in Section 5.6 with the help of same involutory key matrix which was used for encryption. After decryption original image is recovered.

3. Simultaneously, the encrypted message digest is decrypted by using RSA public key presented in Section 3.4 of Chapter 3, to recover message digest.

4. As like encryption, generate the message digest from the image by performing 3-times bit-wise XOR operation.

5. Finally, check for authentication of the recovered message digest and generated message digest.

The encryption and decryption of the proposed system is shown in Figure 5.9 and 5.10 respectively.

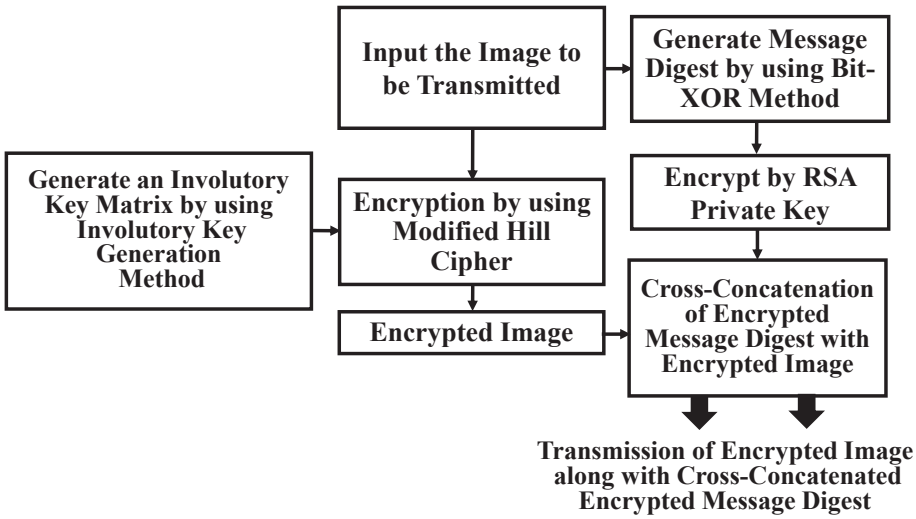


Figure 5.9: Block diagram for encryption

5.7.3 Simulation Results and Discussion

Any security system performs the fundamental security services: confidentiality, authentication, integrity checking and non-repudiation. The proposed cryptosystem satisfies all the security requirements and it is shown in Table 5.5. Figure 5.11 (a) shows a plain/cover image. Figure 5.11 (b) shows the encrypted image. Figure 5.11 (c) and (d) shows the interceptors view of the encrypted image. Figure 5.11(e) shows the decrypted 'Lena' image.

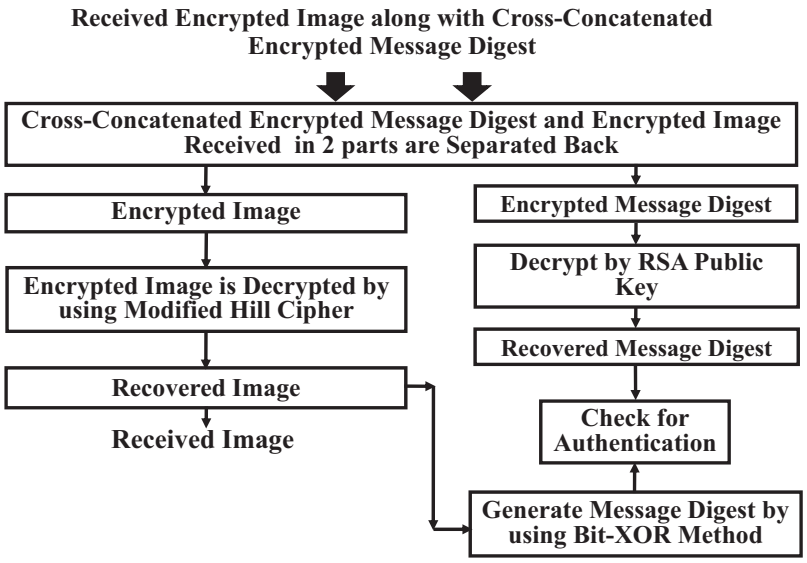


Figure 5.10: Block diagram for decryption

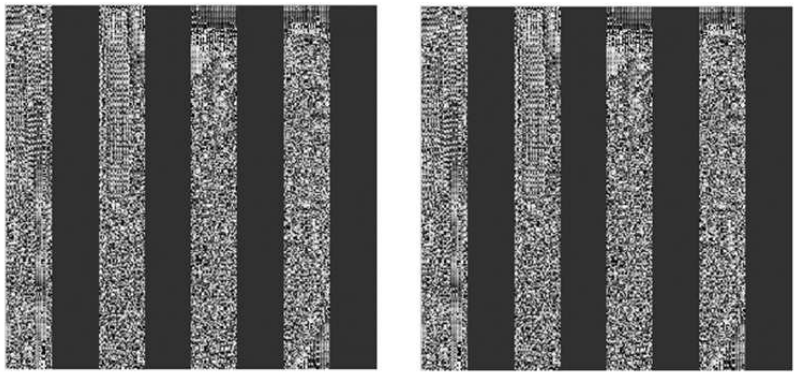
5.8 Summary

In this chapter, a modified Hill cipher is proposed which is the combination of proposed involutory key matrix generation method, modified Hill cipher for a large block of plaintext with interlacing and iteration and robust cryptosystem. This proposed modified Hill cipher takes advantage of all the three methods. Simulation results, security analysis, PSNR and entropy of proposed modified Hill cipher shows the performance superiority of encryption. To acquire the demands of authenticity, integrity and non-repudiation in this chapter a novel hybrid method has also been implemented. This method has employed proposed modified Hill cipher to provide confidentiality. Message digest produced encrypted by private key of RSA algorithm to achieve other features such as authenticity, integrity and non-repudiation.

Table 5.5: Comparative security services

Systems	Confidentiality	Authenticity	Integrity	Non-Repudiation
Message Authentication with Encryption	Yes	Yes	No	No
Message Authentication with Message Digest	No	Yes	Yes	No
Proposed cryptosystem	Yes	Yes	Yes	Yes

(a)



(b)

(c) (d)

(e)

Figure 5.11: (a) Original 'Lena' image, (b) Corresponding cross-concatenated encrypted image, (c) and (d) Interceptor's view, and (e) Corresponding decrypted image

Chapter 6

Secure Image Encryption Using Fingerprint and Password

Chapter 6

Secure Image Encryption Using Fingerprint and Password

Fusion of cryptography and biometrics offers a good security system as human traits are used for generate secret encrypted sources. It is very difficult to crack such secured codes and systems and hence a huge amount of confidential information can be easily secured. Biometrics is gaining popularity for security purposes in many applications. However, during communication and transmission over insecure network channels, there are certain risks of being hacked, modified and reused. Hence, there is a strong need to protect biometrics during communication and transmission [13, 14, 80, 81, 83, 110].

In the present chapter, a biometric cryptosystem approach that combines cryptography and biometrics has been proposed. Under this approach, the image is encrypted with the help of fingerprint and password. A key generated with the combination of fingerprint and password and is used for image encryption. This mechanism is seen to enhance the security of biometrics images during transmission. The proposed method has been validated using simulation studies.

Following this the remaining chapter is organized as follows. Proposed fingerprint feature based biometric cryptosystem is outlined in Section 6.1, where as in Section 6.2, algorithm for proposed biometric cryptosystem is described. The simulation result, security analysis and discussion are presented in Section 6.3 and 6.4 respectively. Finally, a summary of the chapter is presented in Section 6.5.

6.1 Proposed Fingerprint Feature based Biometric Cryptosystem

This section provides the proposed biometric cryptosystem where fingerprint and password is used as a key for encryption and decryption of an image is presented.

6.1.1 Fingerprint Recognition

Fingerprint recognition [111] is one of the best known and most widely used biometric technologies. Automated systems are widely commercially available since the early 1970s. Until recently, fingerprint recognition was used primarily in law enforcement applications. Fingerprint recognition technology extracts features from impressions made by the distinct ridges on the fingertips. The ridge flow exhibits anomalies in local regions of the fingertip, and it is the position and orientation of these anomalies that are used to represent and match fingerprints. Although not scientifically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual. Even identical twins having similar DNA, are believed to have different fingerprints.

6.1.2 Steps for Fingerprint Feature Extraction

According to Bhowmik et al. [87], the main steps for fingerprint feature extraction are as follows.

1. **Image Acquisition:** Fingerprint image can be acquiesced by different types of techniques such as scanners, optical sensor, capacitive sensor or thermal sensor. The images are of poor quality and hence the enhancement step is necessary [87]. Figure 6.1(a) shows the original fingerprint image [87].

2. **Fingerprint Image Enhancement:** The performance of minutiae extraction depends on the fingerprint image quality. In an ideal fingerprint image, ridges and valleys alternate and flow in a locally constant direction. The goal of an enhancement algorithm is to improve the clarity of the ridge structures in the recoverable regions and mark the unrecoverable regions as too noisy for further processing. Different techniques are used for image enhancement. Figure 6.1(b) shows the enhanced fingerprint image [87].

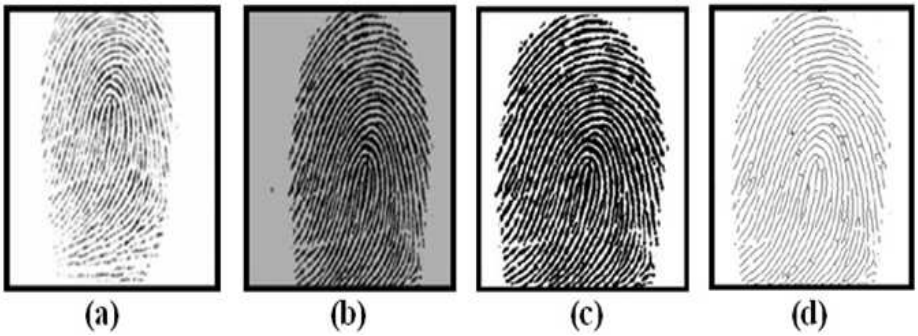


Figure 6.1: (a) Original fingerprint image; (b) Enhanced fingerprint image;(c) Binarized fingerprint image; (d) Thinned fingerprint image

3. **Binarization of Fingerprint Image:**

   This process consist in converting the gray scale image in binary image, i.e, the intensity of the image has only two values: black, representing the ridges, and white, representing the valleys and the background. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of minutiae . A simple method to binarize is to use a global threshold value method where a threshold value is taken and below this all pixels are zero and above this all pixels are 255 that is 1. Figure 6.1(c) shows the binarized fingerprint image [87].

4. **Thinning of Fingerprint Ridges:**

   Thinning is the process applied over binarized image. The objective of thinning is to find the ridges of one pixel width. The process consists in performing successive erosions until a set of connected lines of unit-width is reached while preserving the extent and connectivity of the original shape. These lines are also called skeletons. Sometimes using erosion might cause some features to be corrupted, so another function is used which is called as dilation. Dilation before erosion stores small gaps before thinning the image [111]. Figure 6.1(d) shows the thinned fingerprint image [87]. In this figure, it finds that the rigid lines are representing a line of width one pixel.

5. **Minutiae Extraction:** The image obtained after binarization and thinning is ready to extract the features. If all the white pixels are 1 and black pixels are 0 then the width of the rigid lines of fingerprint is represented by only one zero pixel. In the image each pixel is surrounded by eight pixels and called neighbor pixel. In

any point of a rigid line the summation of the neighbor pixels must be 6. If the rigid line is terminated then the summation will be changed and that will be 7. On the other hand in a point of bifurcation the summation will be 5 [112]. Like that feature extraction occurs from the fingerprint image. The minutias are detected by using 3×3 pattern masks which is as shown in Figure 6.2 [87]. Samples of masks used for identifying the terminations and bifurcations point are shown in Figure 6.3. The formula for knowing of ridge ending and bifurcation points is as follows.

$$P_c = \frac{1}{255} \sum_{i=1}^{8} P_i \tag{6.1}$$

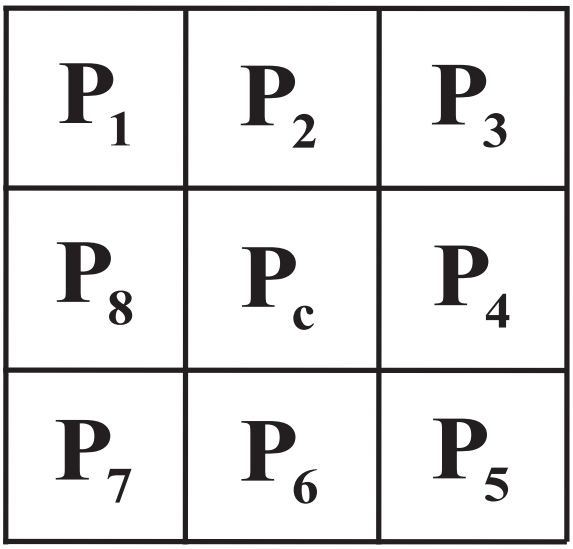


Figure 6.2: 3×3 window for searching minutiae

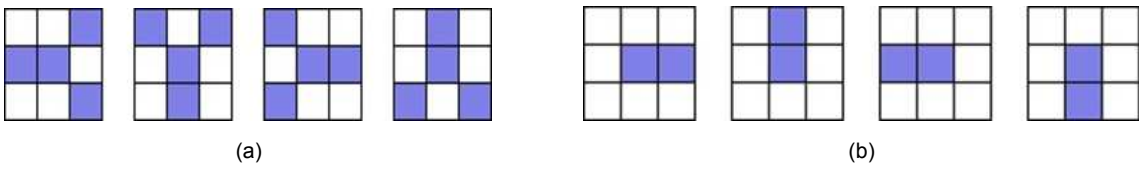


Figure 6.3: (a) Masks for bifurcation detection; (b) Masks for termination detection

6.2 Algorithm for Proposed Biometric Cryptosystem

Figure 6.4 and Figure 6.5 shows the block diagram for encryption and decryption respectively.

6.2.1 Encryption Algorithm

1. Choose a fingerprint image and extract the termination and bifurcation points as T_x,T_y and B_x,B_y respectively.
   where
   T_x represents x-coordinate of the terminator of size $[n \times 1]$.
   T_y represents y-coordinate of the terminator of size $[n \times 1]$.
   B_x represents x-coordinate of the bifurcation of size $[m \times 1]$.
   B_y represents y-coordinate of the bifurcation of size $[m \times 1]$.
   n and m represents the number of terminator and bifurcation points in a biometric fingerprint image template and T_x,T_y,B_x,B_y represents the matrices which can be calculated from the biometric fingerprint image template.
   Suppose there are 10 terminator and 20 bifurcations. Then size of $T_x = [10][1]$, size of $T_y = [10][1]$, size of $B_x = [20][1]$, size of $B_y = [20][1]$.

2. Choose either T_x, B_x or T_y, B_y. Suppose it will be T_x, B_x. The higher sized matrix is used for generating the seed number, denoted as b and the smaller sized matrix is used for generating the multiplying factor, denoted as t, both were used for generating the involutory key matrix, denoted as K.

3. Reshape the derived matrices into square matrices and calculate the determinant of each of the square matrices. Let the determinant of the larger matrix denoted as P, and the determinant of the smaller matrix denoted as Q.

4. Choose a numerical password of any length.

5. Form the polynomial using the password. If the length of the password is 6 digit than polynomial will be Polynomial(x) $= d_1x^5 + d_2x^4 + d_3x^3 + d_4x^2 + d_5x^1 + d_6$ [14, 113, 114].

6. Secret key is to be generated from the polynomial. To generate the secret key take the coefficients of the variable x. Suppose the password is 520304, than

polynomial will be $5x^5 + 2x^4 + 3x^2 + 4$ and the secret key will be 5234.

7. Calculate the square root of the secret key, denoted as S.

8. Calculate seed number, $b = S - P$ and multiplying factor, $t = S - Q$.

9. Generate an involutory key matrix, K which is presented in Section 2.3.7 by using b as the seed number and t as the multiplying factor. In the proposed method, *mod* 256 is used for generating the involutory key matrix.

10. Choose an image which is to be encrypted. Image can be of any size.

11. Now encrypt the image by using the proposed modified Hill cipher algorithm which is presented in Section 5.6.1 and with the involutory key matrix generated in step 9 of this algorithm.

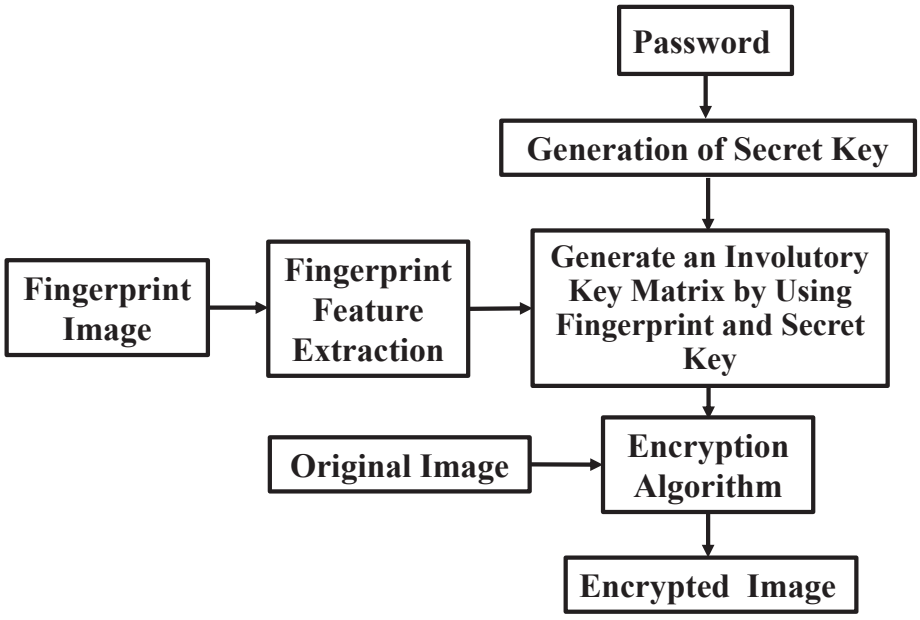


Figure 6.4: Block diagram for encryption

6.2.2 Decryption Algorithm

1. Choose the same fingerprint image and extract the termination and bifurcation points as T_x, T_y and B_x, B_y respectively.

2. Choose either T_x, B_x or T_y, B_y. Suppose it will be T_x, B_x. The higher sized matrix is used for generating the seed number, denoted as b and the smaller sized matrix is used for generating the multiplying factor, denoted as t both were used for generating the involutory key matrix, denoted as K.

3. Reshape the derived matrices into square matrices and calculate the determinant of each of the square matrices. Let the determinant of the larger matrix denoted as P, and the determinant of the smaller matrix denoted as Q.

4. Choose the same password which is used for encryption.

5. Form the polynomial using the password. Secret key is to be generated from the polynomial.

6. Calculate the square root of the secret key, denoted as S.

7. Calculate seed number, $b = S - P$ and multiplying factor, $t = S - Q$.

8. Generate an involutory key matrix, K which is presented in Section 2.3.7 by using b as the seed number and t as the multiplying factor.

9. Take the encrypted image which is obtained from encryption.

10. Now decrypt the encrypted image by using the proposed modified Hill cipher algorithm which is presented in Section 5.6.2 and the generated involutory key matrix of step 8. For decryption, we need K^{-1}. For involutory key matrix, $K^{-1} = K$.

6.3 Simulation Results

Different images are encrypted and decrypted by using the proposed biometric cryptosystem where fingerprint and password as key. The fingerprint feature extraction results are shown in Figure 6.6. The encryption and decryption results of different images by using proposed biometric cryptosystem are shown in Figure 6.7. In Figure 6.7(b, e), it is found that proposed biometric cryptosystem can able to encrypt the images properly. In Figure 6.7(c, f), it shows that there is no loss of data in decryption. So the proposed biometric cryptosystem is applicable to protect both conventional and biometric images during communication and transmission. The

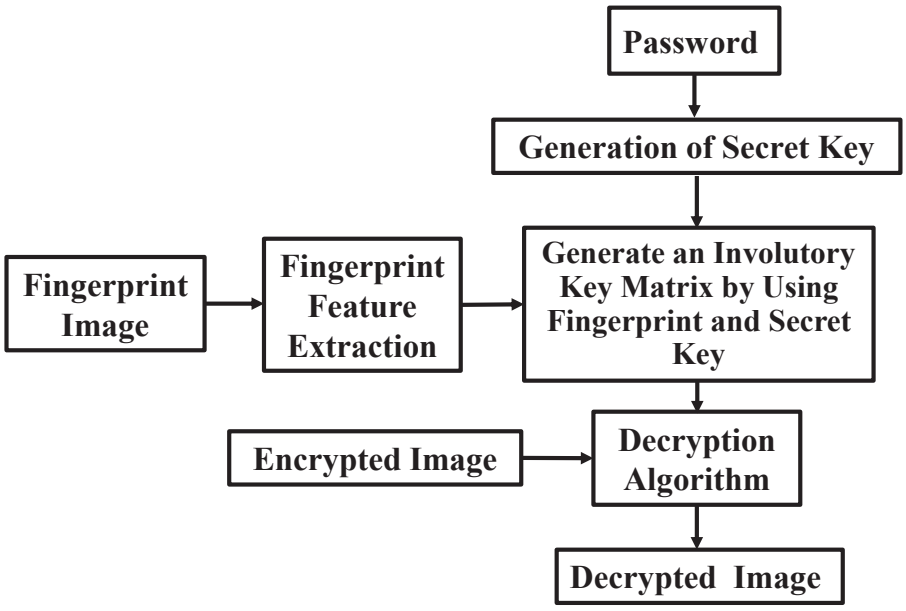


Figure 6.5: Block diagram for decryption

fingerprint image is taken from the CASIA (Chinese Academy of Sciences' Institute of Automation) image database [99]. The eye image is taken from the UBIRIS.v2 database [115].

6.4 Security Analysis and Discussion

Some security analysis has been performed on the proposed encryption technique which includes statistical (histogram, scattered diagram, correlation coefficient) analysis, differential analysis, and entropy measure. The security analyses for the proposed biometric cryptosystem technique are discussed as follows.

6.4.1 Statistical Analysis

Histogram of Encrypted Image:

To resist statistical attack, the histogram of the encrypted images should be uniformly distributed in all gray levels. A detail study has been conducted and the results are summarized as followings. Different images have been tested, and similar results are obtained. Figure 6.8 shows the histogram of original, encrypted, and decrypted images by using proposed biometric cryptosystem technique. It compares the gray histogram of the images before and after encryption to analyze the statistical

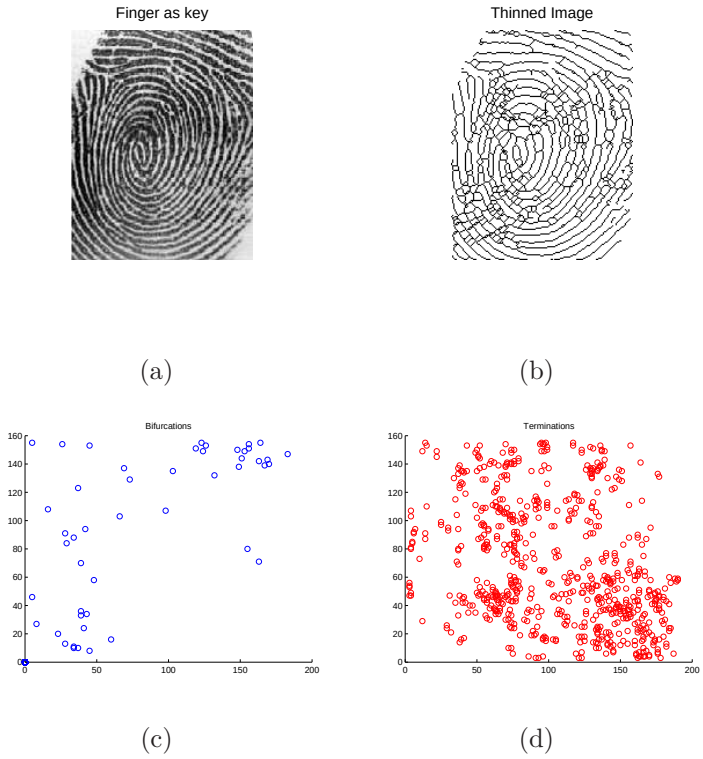
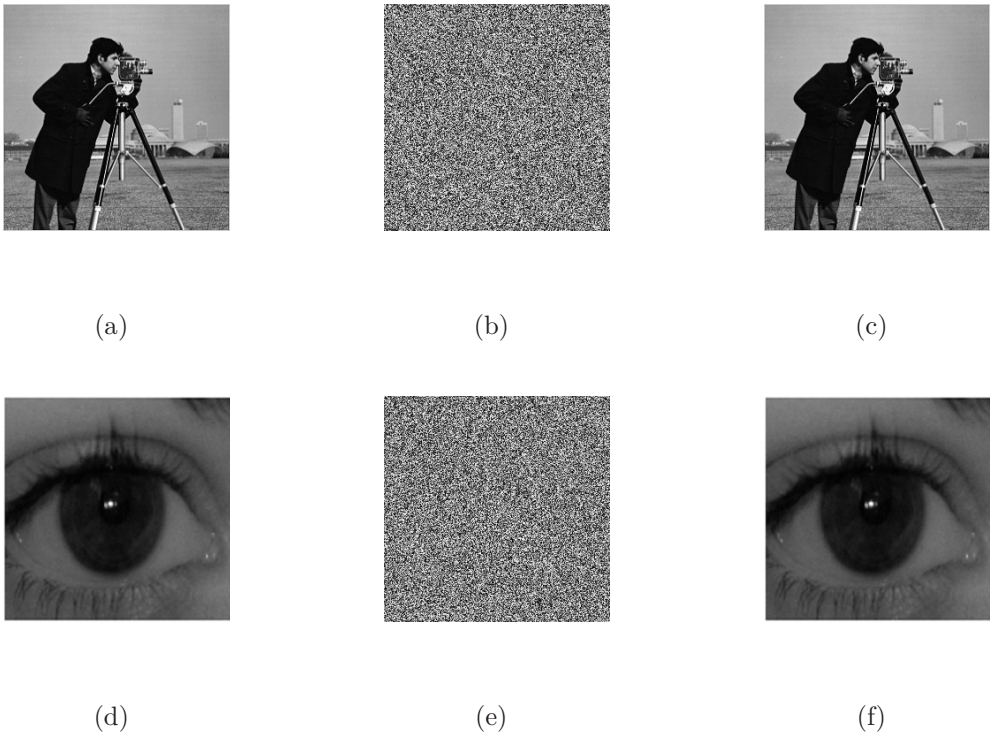


Figure 6.6: (a) Original fingerprint image; (b) Thinned fingerprint image; (c) Bifurcations of fingerprint image; (d) Terminations of fingerprint image.

performance. From Figure 6.8, it is observed that the original pixel gray values are concentrated on some value, but the pixel gray values after the encryption are scattering in the entire pixel value space, namely, two images have lower similarity as a result gives high quality of encryption. Thereby, the proposed cryptosystem has strong ability of resisting statistical attack. Also there is no loss of data in decryption. So the proposed method is applicable to protect both conventional and biometric images during communication and transmission. Figure 6.9(a, c) shows the scattered diagram between original and encrypted images by using the proposed biometric cryptosystem method. It shows that, all the points spread throughout the surface. That means weaker correlation occurs between original and encrypted images. Figure 6.9(b, d) shows the scattered diagram between original and decrypted images using proposed biometric cryptosystem method. It shows that, all the points are along a line. That means stronger correlation occurs between original and decrypted images.



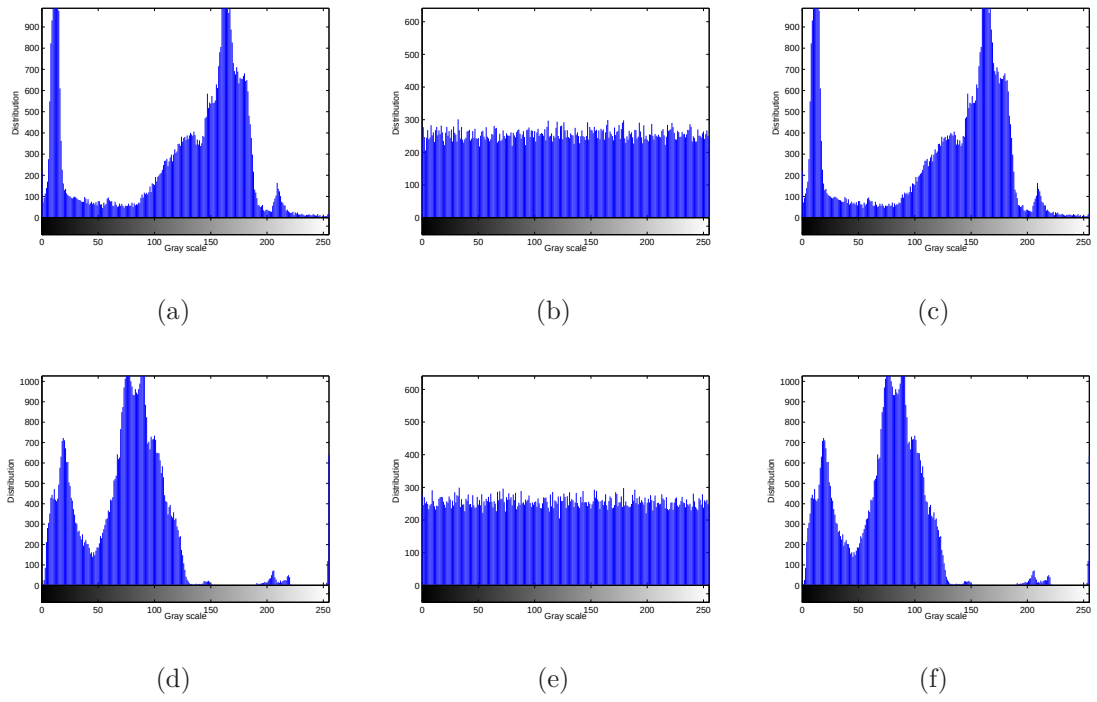
(a) (b) (c)

(d) (e) (f)

Figure 6.7: (a, d) Original 'Cameraman' and 'Eye' images respectively; (b, e) Corresponding encrypted images by using proposed biometric cryptosystem technique; (c, f) Corresponding decrypted images by using proposed biometric cryptosystem technique respectively.

Correlation of Adjacent Pixels

From Table 6.1, it found that the correlation coefficient of the adjacent pixels in the encrypted image is very small, which is close to 0 for the proposed biometric cryptosystem method and original image is almost close to 1. The average correlation coefficient is close to 0 for the proposed method. It clearly be seen that the proposed method can destroy the relativity effectively; the proposed image encryption algorithm has a strong ability to resist statistical attack. Figure 6.10 and 6.11 shows the correlation distribution of two adjacent pixels for 'Cameraman', and 'Eye' images respectively by using the proposed biometric cryptosystem method. From the contrast diagrams of Figure 6.10 and 6.11 it can be observed that the correlation between pixels of original image is much larger than the correlation between pixels of encryption image. That means, the adjacent pixels of original image have very strong linear correlation, while the correlation between adjacent pixels of encrypted image is very small. It has damaged the linear correlation of original image. Therefore the proposed



(a) (b) (c)

(d) (e) (f)

Figure 6.8: (a, d) Histograms of original 'Cameraman' and 'Eye' images respectively, (b, e) Histograms of corresponding encrypted images, (c, f) Histograms of corresponding decrypted images respectively by using proposed biometric cryptosystem technique.

biometric cryptosystem technique can effectively resist pixel correlation statistical attack.

6.4.2 Differential Analysis

The major requirement of all the encryption techniques is the encrypted image should be significantly different to the original one. To quantify the difference between encrypted images and corresponding original images, three measures were used: MAE, NPCR, and UACI. Apart from that, Peak Signal to Noise Ratio (PSNR) is also used to show the efficacy of the method. The comparison of NPCR, UACI, MAE, and PSNR criteria of 'Cameraman' and 'Eye' images by using the proposed biometric cryptosystem is as shown in Table 6.2.

From Table 6.2, it found that, the NPCR value of 'Cameraman' image is equal to the expected NPCR value and 'Eye' image is 0.014% higher than the expected NPCR value. Similarly, the UACI value of 'Cameraman' image and 'Eye' image is nearer equal to the expected UACI value. The MAE values are larger for all the images.

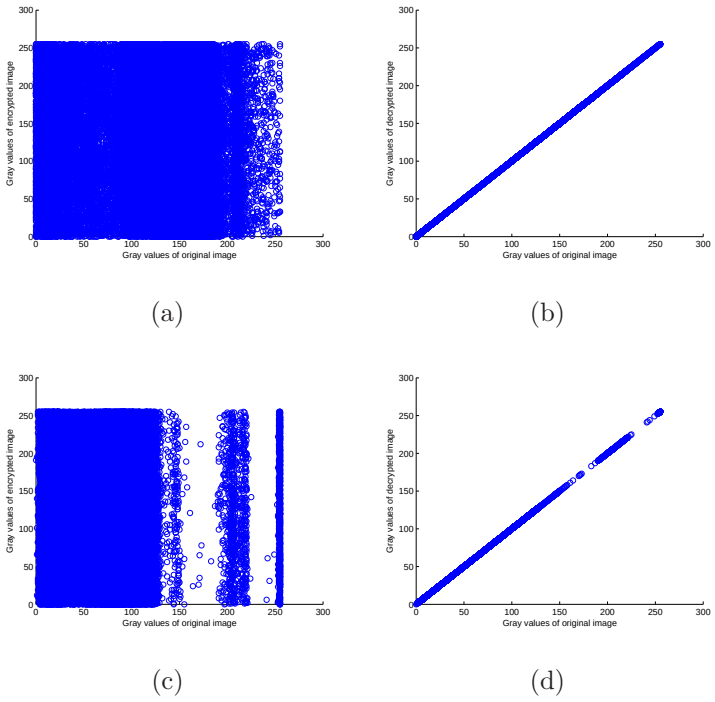


Figure 6.9: (a, c) Scattered diagram between original and encrypted images of 'Cameraman' and 'Eye' respectively by using proposed biometric cryptosystem method, (b, d) Scattered diagram between original and decrypted images of 'Cameraman' and 'Eye' respectively by using proposed biometric cryptosystem technique.

Consequently the PSNR values are smaller for all the images.

6.4.3 Measure of Entropy

The comparison of the entropy between original images and encrypted images using the proposed biometric cryptosystem is presented in Table 6.3. A higher value of the entropy obtained in case of proposed biometric cryptosystem algorithm indicates more randomness in the encrypted image resulting in better encryption.

6.5 Summary

A biometric cryptosystem approach that combines cryptography and biometrics has been proposed and validated using simulation studies. Under this approach, the image is encrypted with a key generated with the combination of fingerprint and

Table 6.1: Correlation coefficient of adjacent pixels of original images and their corresponding encrypted images by using proposed biometric cryptosystem.

Correlation coefficient	Original images		Encrypted images by using the proposed biometric cryptosystem	
	Cameraman	Eye	Cameraman	Eye
Horizontal (H)	0.9203	0.9766	- 0.0098	- 0.0091
Vertical (V)	0.9539	0.9659	- 0.0045	- 0.0040
Diagonal (D)	0.8859	0.9393	0.0053	0.0006
$(H^2 + V^2 + D^2)^{0.5}$	1.5943	1.6641	0.0119	0.0099
Average (H, V, D)	0.9200	0.9606	- 0.0030	- 0.0041

Table 6.2: Comparison of NPCR, UACI, MAE, and PSNR criteria of 'Cameraman' and 'Eye' images by using the proposed biometric cryptosystem technique

Criteria (expected value)		Original image Vs. Encrypted image
NPCR (99.61 %)	Cameraman	99.6078
	Eye	99.6246
UACI (33.46 %)	Cameraman	31.2818
	Eye	32.0858
MAE (larger value)	Cameraman	79.7687
	Eye	81.8188
PSNR (smaller value)	Cameraman	8.3793
	Eye	8.1620

password. Password can be stolen but as this scheme is combination of a biometric trait, it enhances the security enormously. Security analysis of the techniques reveals superiority of encryption and decryption of images.

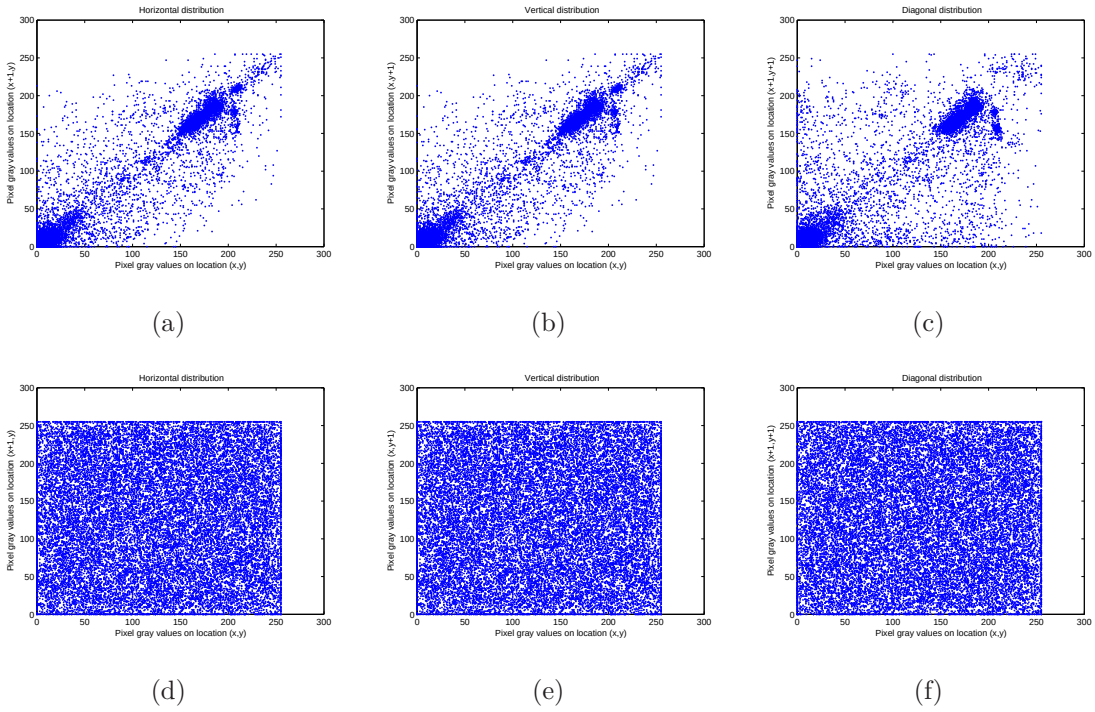


Figure 6.10: Correlation distribution of two adjacent pixels for 'Cameraman' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed biometric cryptosystem technique.

Table 6.3: Entropy between original images and encrypted images by using the proposed biometric cryptosystem technique

Images	Entropy	
	Original images	Encrypted images by the proposed biometric cryptosystem
Cameraman	7.1936	7.9621
Eye	6.8643	7.9561

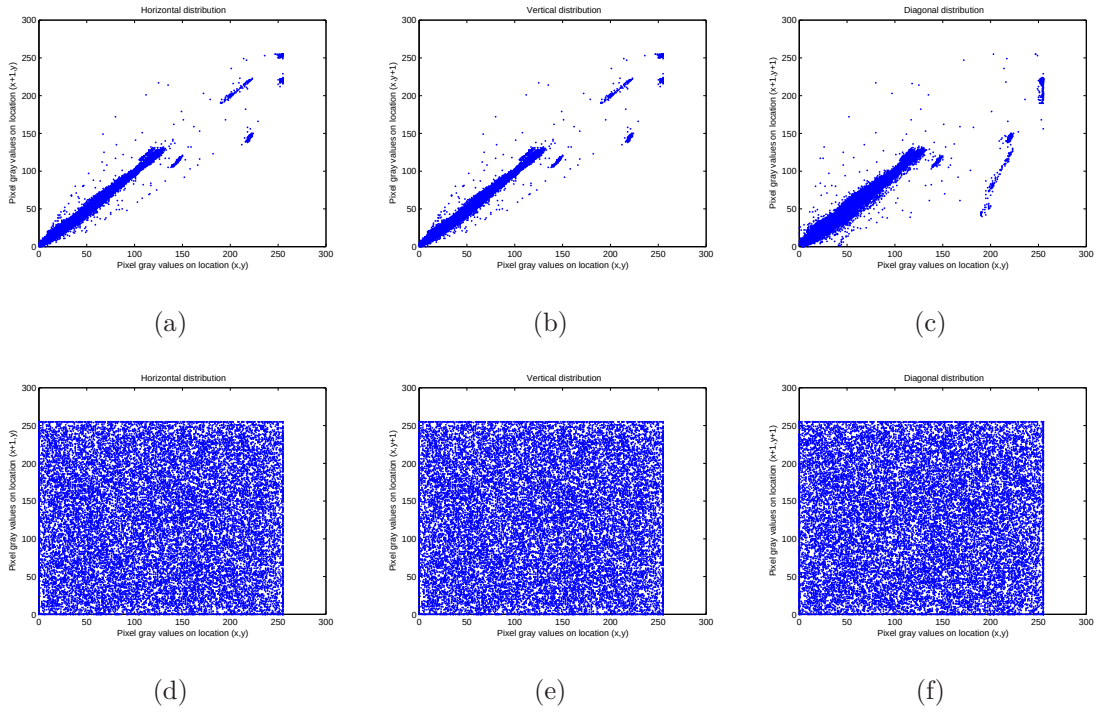


Figure 6.11: Correlation distribution of two adjacent pixels for 'Eye' image: (a, b, c) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation, and diagonal correlation of adjacent pixels of corresponding encrypted image using proposed biometric cryptosystem technique

Chapter 7

Conclusion and Future Work

Chapter 7

Conclusion and Future Work

Confidentiality is the most important requirement for storage and transmission of information. Encryption addresses the need of confidentiality both in storage and transmission. In the last few decades, researchers are working in the field of image encryption. The problem area is still open due to new threats and needs substantial research.

In this thesis, attempts have been made to design few encryption techniques for image. Chapter 2 discussed invertible, involutory, and permutation key matrix generation methods for Hill cipher. Invertible, involutory matrix generation method solves the key matrix inversion problem. Permutation key matrix generation method enhancement increases the Hill system's security considerably. Moreover, involutory matrix eliminates necessity of matrix inverse for Hill decryption. This meant that same machinery could be used both for encryption and decryption of massages; no additional hardware would be needed to compute inverses before decrypting. Moreover the algorithm can generate the different key matrix for each block encryption instead of keeping the key matrix constant. This increases the secrecy of data. The conventional Hill cipher technique fails to encrypt images properly if the image consists of large area covered with same colour or gray level. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. To address these issues two different techniques are proposed, those are advanced Hill Cipher algorithm and H-S-X cryptosystem to encrypt the images properly. Comparative study with conventional Hill cipher, Security analysis and Entropy study between original images and encrypted images by using the proposed techniques reveals superiority of encryption and decryption of images. On the other hand, H-S-X

cryptosystem has been used to instil more diffusion and confusion on the cryptanalysis. FPGA implementation of both the proposed techniques has been carried out. Image encryption using Hill cipher algorithm has also been implemented using systolic arrays on FPGA. Performance analysis with conventional multiplier, Booth Wallace multiplier and vedic multiplier in processing element of systolic array separately has been completed to verify the performance of the Hill cipher implementation. Comparative analysis reveals that Vedic multiplier uses a less number of adders in implementation of Hill Cipher. The comparative analysis with respect to FPGA utilization, power and Speed of operation shows that vedic multipliers are faster and consume more power than Booth Wallace multiplier in Hill cipher Implementation. The comparative analysis with respect to FPGA utilization, power and speed of operation shows that Vedic multiplier is high performance architecture in advance Hill cipher implementation.

An extended Hill cipher algorithm based on XOR and zigzag operation is proposed in chapter 3 to encrypt both conventional and biometric images. The comparative analysis revealed that in the proposed technique the encryption and decryption time are reduced as compared to some of the works [50, 52]. The simulation result also shows that there is no data lost during encryption. In the proposed scheme the safe time is calculated as very long time to find the key matrix. So the proposed technique is more resistant to intruder attack. Then, a hybrid cryptosystem is implemented in chapter 3 by using RSA algorithm and proposed extended Hill cipher technique to take the advantages of both the techniques. The RSA algorithm solves the key distribution problem and the proposed extended Hill cipher algorithm gives a high quality of encryption with less encryption and decryption time.

Due to some intrinsic features of images, some of the traditional encryption schemes are generally not suitable for image encryption. To achieve an excellent level of image encryption and to create great disorder between the pixels of the images in chapter 4, two distinct approaches for image encryption such as,

- Chaos based DNA coding along with shifting and scrambling
- Chaos based DNA coding along with poker shuffle

have been proposed. The comparison analysis based on different considerations such as images and text used, security analysis revealed that the proposed techniques have greater outputs as compared to other literature reported. The simulation results of both the methods show that the original images and their corresponding

histogram images have lower similarity. Therefore, both the proposed algorithms have strong ability to resist statistical attack. The comparison result of histograms of the encrypted images shows that the histogram of encrypted image using poker shuffling is wide and well spread throughout the dynamic range of the image as compared to the histogram of encrypted image using shifting and scrambling. Finally the FPGA implementation of the proposed chaos based DNA coding along with shifting and scrambling technique has been carried out.

A modified Hill cipher which is the combination of proposed involutory key matrix generation method, Sastry et al's [51] modified Hill cipher for a large block of plaintext with interlacing and iteration, and Rushdi et al's [24] robust cryptosystem was proposed in chapter 5. This modified Hill cipher takes advantages of all the three techniques. Modified Hill cipher using interlacing and iteration cannot be used for encrypting an image because of the loss of data during interlacing (binary conversion and rearrangement) of temporary cipher though it provides a robust encryption. So the modified Hill cipher with interlacing and iteration combined with Involutory key matrix eliminates the possibility of any decimal value and makes the modified Hill cipher evenly applicable to images too. To create a more secure algorithm which resists known plaintext attack Rushdi et al's [24] cryptosystem is combined with the other two. Finally, in this chapter to acquire the demands of authenticity, integrity and non-repudiation, a novel hybrid method has been implemented along with proposed modified Hill cipher algorithm. The proposed modified Hill cipher is employed to provide confidentiality. Message digest encrypted by the private key of the RSA algorithm achieves other features such as authenticity, integrity and non-repudiation. Performance and security analysis show that the proposed scheme meets all the four cryptographic goals and is more secure.

A biometric cryptosystem approach that combines cryptography and biometrics has been presented and validated using simulation studies in Chapter 6. Under this approach, the image is encrypted with a key generated with the combination of fingerprint and password. Password can be stolen but as this scheme is combination of a biometric trait, it enhances the security enormously. Security analysis of the techniques revealed superiority of encryption and decryption of images.

Scope for Further Research

The research findings made out of this thesis has opened several research directions, which have a scope for further investigations. The proposed schemes mostly deal gray scale images, which can be extended to color images. In this thesis, cryptographic approach used to encrypt biometric images. Encrypted images are stored in cryptographic protected system. Cryptography is not much suitable for high speed matching since decryption of biometric image is required before matching. Further to develop high speed, robust and efficient image encryption techniques will be an interesting direction of research.

Bibliography

[1] W. Stallings, *Cryptography and network security: principles and practice*, 4th ed., ser. The William Stallings Books on Computer and Data Communications. Pearson Prentice Hall, 2006.

[2] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley and Sons, 2007.

[3] B. Forouzan, *Introduction to cryptography and network security*, ser. McGraw-Hill Forouzan networking series. McGraw-Hill Higher Education, 2008.

[4] R. A. Rueppel, "Stream ciphers," in *Analysis and Design of Stream Ciphers*. Springer, 1986, pp. 5–16.

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[6] G. Xiao, M. Lu, L. Qin, and X. Lai, "New field of cryptography: DNA cryptography," *Chinese Science Bulletin*, vol. 51, no. 12, pp. 1413–1420, 2006.

[7] X. Wang and J. Zhang, "An image scrambling encryption using chaos-controlled poker shuffle operation," in *International Symposium on Biometrics and Security Technologies*. IEEE, 2008, pp. 1–6.

[8] J. Zou, R. K. Ward, and D. Qi, "A new digital image scrambling method based on Fibonacci numbers," in *Proceedings of the International Symposium on Circuits and Systems*, vol. 3. IEEE, 2004, pp. III–965.

[9] J. Fridrich, "Image encryption based on chaotic maps," in *IEEE International Conference on Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation*, vol. 2. IEEE, 1997, pp. 1105–1110.

[10] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[11] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons and Fractals*, vol. 38, no. 1, pp. 213–220, 2008.

[12] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, pp. 113:1–113:17, 2008.

[13] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of biometrics*. Springer Science and Business Media, 2007.

[14] M. Kaur, S. Sofat, and D. Saraswat, "Template and database security in biometrics systems: a challenging task," *International Journal of Computer Applications*, vol. 4, no. 5, pp. 1–5, 2010.

[15] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, 1929.

[16] ——, "Concerning certain linear transformation apparatus of cryptography," *The American Mathematical Monthly*, vol. 38, pp. 135–154, 1931.

[17] R. Cooper, "Linear transformations in galois fields and their application to cryptography," *Cryptologia*, vol. 4, no. 3, pp. 184–188, 1980.

[18] W. A. Kiele, "A tensor-theoretic enhancement to the Hill cipher system," *Cryptologia*, vol. 14, no. 3, pp. 225–233, 1990.

[19] W. T. Jeffrey Overbey and J. Wojdylo, "On the keyspace of the Hill cipher," *Cryptologia*, vol. 29, no. 1, pp. 59–72, 2005.

[20] D. H. Ismail I.A., Amin M., "How to repair the Hill cipher," *J. Zhejiang University Science*, vol. 7, no. 12, pp. 2022–2030, 2006.

[21] S. Saeednia, "How to make the Hill cipher secure," *Cryptologia*, vol. 24, no. 4, pp. 353–360, 2000.

[22] C. H. Lin, C.-Y. Lee, and C.-Y. Lee, "Comments on Saeednia's improved scheme for the Hill cipher," *Journal of the Chinese institute of engineers*, vol. 27, no. 5, pp. 743–746, 2004.

[23] A. Chefranov, "Secure Hill cipher modification SHC-M," in *Proceedings of the First International Conference on Security of Information and Networks (SIN2007), Gazimagusa (TRNC) North Cyprus, Canada*. Trafford Publishing, 2007, pp. 34–37.

[24] M. F. Rushdi A. Hamamreh, "Design of a robust cryptosystem algorithm for non-invertible matrices based on Hill cipher," *International Journal of Computer Science and Network Security*, vol. 9, no. 5, pp. 11–16, 2009.

[25] A. Y. Mahmoud and A. G. Chefranov, "Hill cipher modification based on eigenvalues HCM-EE," in *Proceedings of the 2nd international conference on Security of information and networks*. ACM, 2009, pp. 164–167.

[26] A. Mahmoud and A. Chefranov, "Hill cipher modification based on pseudo-random eigenvalues," *Applied Mathematics*, vol. 8, no. 2, pp. 505–516, 2014.

[27] A. Mahmoud and A. G. Chefranov, "Secure Hill cipher modification based on generalized permutation matrix SHC-GPM," *Information Sciences Letters*, pp. 91–102, 2012.

[28] H. T. Kung, "Why systolic architectures?" *IEEE computer*, vol. 15, no. 1, pp. 37–46, 1982.

[29] S. K. Jain, L. Song, and K. K. Parhi, "Efficient semisystolic architectures for finite-field arithmetic," *IEEE Transaction Very Large Scale Integr. Syst.*, vol. 6, no. 1, pp. 101–113, Mar. 1998.

[30] G. Saldana and M. Arias-Estrada, "Compact FPGA-based systolic array architecture suitable for vision systems," *International Journal of High Performance Systems Architecture*, vol. 1, no. 2, pp. 124–132, 2007.

[31] A. D. Booth, "A signed binary multiplication technique," *The Quarterly Journal of Mechanics and Applied Mathematics*, vol. 4, no. 2, pp. 236–240, 1951.

[32] J. Fadavi-Ardekani, "M × N Booth encoded multiplier generator using optimized Wallace trees," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 1, no. 2, pp. 120–125, 1993.

[33] P. E. Madrid, B. Millar, and E. E. Swartzlander, "Modified Booth algorithm for high radix fixed-point multiplication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 1, no. 2, pp. 164–167, 1993.

[34] R. Katti, "A modified Booth algorithm for high radix fixed-point multiplication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 2, no. 4, pp. 522–524, 1994.

[35] S. J. Jou, M. H. Tsai, and Y. L. Tsao, "Low-error reduced-width Booth multipliers for DSP applications," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 11, pp. 1470–1474, 2003.

[36] S. R. Kuang, J. P. Wang, and C. Y. Guo, "Modified Booth multipliers with a regular partial product array," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 56, no. 5, pp. 404–408, 2009.

[37] D. P. Chaudhary V.N, "Analysis and implementation of low power Wallace tree multiplier," *Journal of Information, Knowledge and Research in Electronics and Communication Engineering*, vol. 01, no. 02, 2010.

[38] N. K. Gahlan, P. Shukla, and J. Kaur, "Implementation of Wallace tree multiplier using compressor." *International Journal of Computer Technology and Applications*, vol. 3, no. 3, 2012.

[39] M. Rao and S. Dubey, "A high speed and area efficient Booth recoded wallace tree multiplier for fast arithmetic circuits," in *Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia)*, 2012, pp. 220–223.

[40] G. G. Kumar and V. Charishma, "Design of high speed vedic multiplier using vedic mathematics techniques," *International Journal of Scientific and Research Publications*, vol. 2, no. 3, p. 1, 2012.

[41] P. Saha, A. Banerjee, A. Dandapat, and P. Bhattacharyya, "Design of high speed vedic multiplier for decimal number system," in *Progress in VLSI Design and Test*. Springer, 2012, pp. 79–88.

[42] S. M. Qasim, A. A. Telba, and A. Y. AlMazroo, "FPGA design and implementation of matrix multiplier architectures for image and signal processing applications," *International Journal of Computer Science and Network Security*, vol. 10, no. 2, pp. 168–176, 2010.

[43] J. Hormigo, G. Caffarena, J. P. Oliver, and E. Boemo, "Self-reconfigurable constant multiplier for FPGA," *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 6, no. 3, p. 14, 2013.

[44] M. R. Pillmeier, M. J. Schulte, and E. G. Walters III, "Design alternatives for barrel shifters," in *International Symposium on Optical Science and Technology*. International Society for Optics and Photonics, 2002, pp. 436–447.

[45] A. Asati and C. Shekhar, "A purely MUX based high speed barrel shifter vlsi implementation using three different logic design styles," in *Mechanical Engineering and Technology*. Springer, 2012, pp. 639–646.

[46] V. Sastry and V. Janaki, "On the modular arithmetic inverse in the cryptology of Hill cipher," in *Proceedings of North American Technology and Business Conference*, 2005, p. 105.

[47] V. Sastry, S. U. Kumar *et al.*, "A large block cipher using modular arithmetic inverse of a key matrix and mixing of the key matrix and the plaintext," *Journal of Computer Science*, vol. 2, no. 9, p. 698, 2006.

[48] V. Sastry and V. Janaki, "A block cipher using linear congruences," *Journal of Computer Science*, vol. 3, no. 7, p. 556, 2007.

[49] V. Sastry and N. R. Shankar, "Modified Hill cipher with interlacing and iteration," *Journal of Computer Science*, vol. 3, no. 11, p. 854, 2007.

[50] V. Sastry, "Modified Hill cipher with key dependent permutation and circular rotation," *Journal of Computer Science*, vol. 3, no. 9, p. 736, 2007.

[51] V. Sastry and N. R. Shankar, "Modified Hill cipher for a large block of plaintext with interlacing and iteration," *Journal of Computer Science*, vol. 4, no. 1, pp. 15–20, 2008.

[52] V. U. Sastry, N. R. Shankar, and S. D. Bhavani, "A modified Hill cipher involving interweaving and iteration." *IJ Network Security*, vol. 10, no. 3, pp. 210–215, 2010.

[53] P. K. Naskar and A. Chaudhuri, "A secure symmetric image encryption based on bit-wise operation," *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, vol. 6, no. 2, p. 30, 2014.

[54] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31–38, 2011.

[55] F. Belkhouche and U. Qidwai, "Binary image encoding using 1D chaotic maps," in *IEEE Region 5, 2003 Annual Technical Conference.* IEEE, 2003, pp. 39–43.

[56] G. Gu and G. Han, "An enhanced chaos based image encryption algorithm," in *First International Conference on Innovative Computing, Information and Control*, vol. 1. IEEE, 2006, pp. 492–495.

[57] H.-P. Xiao and G. J. Zhang, "An image encryption scheme based on chaotic systems," in *International Conference on Machine Learning and Cybernetics.* IEEE, 2006, pp. 2707–2711.

[58] I. A. Ismail, M. Amin, and H. Diab, "A digital image encryption algorithm based a composition of two chaotic logistic maps." *IJ Network Security*, vol. 11, no. 1, pp. 1–10, 2010.

[59] K. Faraoun, "Chaos-based key stream generator based on multiple maps combinations and its application to images encryption." *Int. Arab J. Inf. Technol.*, vol. 7, no. 3, pp. 231–240, 2010.

[60] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.

[61] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied soft computing*, vol. 11, no. 1, pp. 514–522, 2011.

[62] N. Sethi and S. Vijay, "Comparative image encryption method analysis using new transformed-mapped technique," in *Proceedings of the Conference on Advances in Communication and Control Systems-2013*. Atlantis Press, 2013.

[63] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," *Multimedia Tools and Applications*, pp. 1–31, 2013.

[64] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Image encryption using random bit sequence based on chaotic maps," *Arabian Journal for Science and Engineering*, vol. 39, no. 2, pp. 1039–1047, 2014.

[65] J. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 3, pp. 578–588, 2014.

[66] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[67] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in *Aspects of Molecular Computing*. Springer, 2004, pp. 167–188.

[68] Q. Wang, Q. Zhang, and C. Zhou, "A multilevel image encryption algorithm based on chaos and DNA coding," in *Fourth International Conference on Bio-Inspired Computing*. IEEE, 2009, pp. 1–5.

[69] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11, pp. 2028–2035, 2010.

[70] Q. Zhang, X. Xue, and X. Wei, "A novel image encryption algorithm based on DNA subsequence operation," *The Scientific World Journal*, vol. 2012, 2012.

[71] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[72] H. Liu, X. Wang *et al.*, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457–1466, 2012.

[73] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and DNA sequence," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 57–70, 2014.

[74] S. Som, A. Kotal, A. Chatterjee, S. Dey, and S. Palit, "A colour image encryption based on DNA coding and chaotic sequences," in *1st International Conference on Emerging Trends and Applications in Computer Science (ICETACS)*. IEEE, 2013, pp. 108–114.

[75] M. Babaei, "A novel text and image encryption method based on chaos theory and DNA computing," *Natural Computing*, vol. 12, no. 1, pp. 101–107, 2013.

[76] F. A. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul 1999.

[77] M. I. Jabiullah, M. Z. Sarker, A. Rahman, and M. L. Rahman, "A secured message transaction approach by dynamic Hill cypher generation and message digest concatenation," *Daffodil International University Journal of Science and Technology*, vol. 5, no. 1, pp. 62–66, 2010.

[78] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[79] K. Kurosawa and Y. Desmedt, "A new paradigm of hybrid encryption scheme," in *Advances in Cryptology–Crypto 2004*. Springer, 2004, pp. 426–442.

[80] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[81] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[82] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 103–117, 2010.

[83] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 255–268, 2012.

[84] S. Cheepchol, W. San-Um, S. Kiattisin, and A. Leelasantitham, "Digital biometric facial image encryption using chaotic cellular automata for secure image storages," in *4th Joint International Conference on Information and*

Communication Technology, Electronic and Electrical Engineering (JICTEE). IEEE, 2014, pp. 1–5.

[85] I. Marqués and M. Graña, "Image security and biometrics: A review," in *Hybrid Artificial Intelligent Systems*. Springer, 2012, pp. 436–447.

[86] J. Leon, G. Sanchez, G. Aguilar, L. Toscano, H. Perez, and J. Ramirez, "Fingerprint verification applying invariant moments," in *IEEE International Midwest Symposium on Circuits and Systems*, Aug 2009, pp. 751–757.

[87] P. Bhowmik, K. Bhowmik, M. N. Azam, and M. W. Rony, "Fingerprint image enhancement and it's feature extraction for recognition," *International Journal of Scientific & Technology Research*, vol. 1, no. 5, 2012.

[88] U. Rajanna, A. Erol, and G. Bebis, "A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion," *Pattern Analysis and Applications*, vol. 13, no. 3, pp. 263–272, 2010.

[89] G. Bhatnagar, Q. J. Wu, and B. Raman, "A new fractional random wavelet transform for fingerprint security," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 42, no. 1, pp. 262–275, 2012.

[90] G. Bhatnagar and Q. J. Wu, "Chaos-based security solution for fingerprint data during communication and transmission," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 4, pp. 876–887, 2012.

[91] G. bhatnagar and Q. J. Wu, "Enhancing the transmission security of biometric images using chaotic encryption," *Multimedia systems*, vol. 20, no. 2, pp. 203–214, 2014.

[92] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *Signal Processing Magazine*, vol. 30, no. 2, pp. 42–52, 2013.

[93] C. A. Sun, Z. Wang, and G. Wang, "A property-based testing framework for encryption programs," *Frontiers of Computer Science*, vol. 8, no. 3, pp. 478–489, 2014.

[94] P. K, "Notes on number theory and cryptography," http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf, 2000.

[95] D. R. Stinson, *Cryptography: theory and practice*. CRC press, 2005.

[96] A. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," *Physica D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638–2648, 2008.

[97] S. Borujeni and M. Eshghi, "Design and simulation of encryption system based on PRNG and Tompkins-Paige permutation algorithm using VHDL," in *Proceedings of the International Conference on Robotics, Vision, Information and Signal Processing*, 2007, pp. 63–67.

[98] S. Etemadi Borujeni and M. Eshghi, "Chaotic image encryption design using Tompkins-Paige algorithm," *Mathematical Problems in Engineering*, vol. 2009, 2009.

[99] CASIA palmprint database. [Online]. Available: http://biometrics.idealtest.org/

[100] Atul Kahate, *Cryptography and network security.* TMH Education Pvt. Ltd, 2006.

[101] S. Palnitkar, *Verilog HDL: a guide to digital design and synthesis.* Prentice Hall Professional, 2003, vol. 1.

[102] S. Kilts, *Advanced FPGA design: architecture, implementation, and optimization.* John Wiley & Sons, 2007.

[103] The yale face database. [Online]. Available: http://www.vision.ucsb.edu/content/yale-face-database

[104] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759–765, 2005.

[105] F. Zhou, G. Cao, and B. Li, "Design of digital image encryption algorithm based on compound chaotic system," *Journal of Hardin Institute of Technology*, vol. 14, no. 2, pp. 30–33, 2007.

[106] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

[107] J. S. Kilby, "Semiconductor solid circuits," *American Rocket Society 14th Annual Meeting*, 1959.

[108] ——, "Invention of the integrated circuit," *IEEE Transactions on Electron Devices*, vol. 23, no. 7, pp. 648–654, 1976.

[109] B. Schneier, "Cryptanalysis of MD5 and SHA: Time for a new standard," *Computer World*, 2004.

[110] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.

[111] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science and Business Media, 2009.

[112] G. Aguilar, G. Sanchez, K. Toscano, M. Salinas, M. Nakano, and H. Pérez, "Fingerprint recognition," in *Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on*. IEEE, 2007, pp. 32–32.

[113] M. AlTarawneh, W. Woo, and S. Dlay, "Fuzzy vault crypto biometric key based on fingerprint vector features," in *Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on*. IEEE, 2008, pp. 452–456.

[114] D. Moon, W.-Y. Choi, K. Moon, and Y. Chung, "Fuzzy fingerprint vault using multiple polynomials," in *Consumer Electronics, 2009. ISCE'09. IEEE 13th International Symposium on*. IEEE, 2009, pp. 290–293.

[115] H. Proenca, S. Filipe, R. Santos, J. Oliveira, and L. Alexandre, "The UBIRIS.v2: A database of visible wavelength images captured on-the-move and at-a-distance," *IEEE Trans. PAMI*, vol. 32, no. 8, pp. 1529–1535, August 2010.

Dissemination

Journals

1. **Bibhudendra Acharya**, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy, "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm", *International Journal of Security, CSC Journals, ISSN: 1985-2320, Vol. 1, Issue 1, pp. 14-21*, 2007.

2. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher System", *International Journal of Recent Trends in Engineering (Computer Science)*, International Journal of Recent Trends in Engineering (Electrical and Electronics), Vol. 1, No. 4, pp.106-108, 2009.

3. **Bibhudendra Acharya**, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", *International Journal of Recent Trends in Engineering (Computer Science)*, Vol. 1, No. 1, pp. 663-667, 2009.

4. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "A Multilevel Image Encryption Based on Chaos, DNA Coding and Poker Shuffle", Paper under preparation.

5. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption by Using Extended Hill Cipher Algorithm and It's FPGA Implementation", Paper under preparation.

6. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "Novel Secured Image Transaction and Authentication Scheme", Paper under preparation.

Conferences

1. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption by Novel Cryptosystem Using Matrix Transformation", *Proceeding*

of the 1st International Conference on Emerging Trends in Engineering and Technology (ICETET-08), July 16-18, pp. 77-81, 2008, Nagpur, India. DOI: http://doi.ieeecomputersociety.org/10.1109/ICETET.2008.110

2. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "A Novel Cryptosystem Using Matrix Transformation", *Proceedings of SPIT-IEEE Colloquium and International Conference. Vol. 4, pp. 92-95*, 2008.

3. **Bibhudendra Acharya**, Girija Sankar Rath, and Sarat Kumar Patra, "Novel Modified Hill Cipher Algorithm", *Proceedings of International Conference on Emerging Technologies and Applications in Engineering, Technology and Sciences (ICETAETS-08). Vol. 2, pp. 126-130*, 2008.

4. **Bibhudendra Acharya**, Sarat Kumar Patra, and Ganapati Panda, "Novel Hybrid Cryptosystem Using Extended Hill Cipher", *Proceeding of the 3rd International conference on Advanced Computing and Communication Technologies [ICACCT-2008], Panipat, Haryana, India*, 08–09 November 2008.

5. **Bibhudendra Acharya**, Debasish Jena, Sarat Kumar Patra, and Ganapati Panda, "Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System", *Proceeding of International Conference on Advanced Computer Control 2009 (ICACC 2009), Singapore, pp.410-414*, January 22-24, 2009. DOI: http://doi.ieeecomputersociety.org/10.1109/ICACC.2009.101.

6. **Bibhudendra Acharya**, Sambit Kumar Shukla, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "H-S-X Cryptosystem and Its Application to Image Encryption", *Proceeding of International Conference on Advances in Computing, Control, and Telecommunication Technologies (ACT-2009), Trivandrum, Kerala, India, pp. 720-724*, 28-29 December 2009. DOI: http://doi.ieeecomputersociety.org/10.1109/ACT.2009.183.

7. **Bibhudendra Acharya**, Mohammad Imroze Khan, Sarat Kumar Patra, and Ganapati Panda, "Implementation of Hybrid Cryptosystem Using Non-Invertible Matrices Based on Hill Cipher and RSA Algorithm", *Proceeding of National Conference on information and Communication Technology (NCICT-2011), Ewing Christian College (Autonomous College of Allahabad University), Allahabad, India. pp. 21-25*, 5-6 March 2011. (ISSN: 978-93-80697-77-2).

Bibhudendra Acharya

Assistant Professor
Department of Electronics and Telecommunication Engineering
National Institute of Technology Raipur
G.E. Road, Raipur- 492010
Chhatisgarh, India

Ph: +91-7714054882, +91-9907445868

e-mail: bacharya.etc@nitrr.ac.in, bibhudendra@gmail.com

Date of Birth

30 June 1978

Permanent Address

Chandramanipeta Street, Gate Bazar
Berhampur– 760 001, Odisha, India.

Qualification

- Ph.D. (Continuing)
  NIT Rourkela, Orissa, India
- M.Tech. (Telematics & Signal Processing)
  NIT Rourkela, Orissa, India
- B.E. (E&TC)
  Dr. B. A. Marathawada University, Maharastra
- Diploma (ECE)
  MEI Polytechnique, Bangalore, Karnataka
- 10th
  Board of Secondary Education, Orissa

Publications

- 10 Journal Articles
- 26 Conference Papers